UNIVERSITÀ DEGLI STUDI DI GENOVA

DIPARTIMENTO DI GIURISPRUDENZA

Corso di Dottorato in Diritto – Curriculum Pubblicistico

XXXVI Ciclo

Social network e giustizia penale

Nuovi scenari investigativi e probatori

Tutor e Responsabile del Curriculum

Chiar.mo Prof. Mitja Gialuz

Candidato:

Dott. Alessandro Malacarne

Anno Accademico 2022-2023

Agli amici di *sempre*,
e a coloro che ci sono *sempre*

INDICE

PARTE II
"RETI SOCIALI VIRTUALI" TRA PREVENZIONE E INVESTIGAZIONE

CAPITOLO I
ATTIVITÀ *LATO SENSU* INVESTIGATIVE E NUOVE DECLINAZIONI DEI DIRITTI FONDAMENTALI DELLA PERSONA NEI *SOCIAL WEBSITES*

CAPITOLO II
LE INDAGINI SU "FONTI PUBBLICAMENTE ACCESSIBILI" NEL PANORAMA ITALIANO: IL *SOCIAL NETWORK PATROLLING*

CAPITOLO III

LE INVESTIGAZIONI *OPEN ACCESS* NEL SISTEMA DELLA CORTE PENALE INTERNAZIONALE

CAPITOLO IV

FALSE FRIENDS TECHNIQUE E ACQUISIZIONE DI "DATI RISTRETTI"

CAPITOLO V

CAPTAZIONE E APPRENSIONE DELLE "INFORMAZIONI SEGRETE" CONTENUTE NELLE PIATTAFORME DIGITALI

PARTE III
L'IRRUZIONE DEI *SOCIAL NETWORK* NEL PROCESSO PENALE

CAPITOLO I
L'APPROCCIO STRANIERO ALLA *SOCIAL NETWORK EVIDENCE*: L'ESPERIENZA STATUNITENSE

CAPITOLO II
LA PROSPETTIVA ITALIANA

Introduzione
Ragioni dell'analisi e delimitazione dello studio

Se è vero, come ebbe a constatare un illustre processualista del XX secolo, che «è pessima "teoria" quella che non si basa su fatti e fenomeni reali»[1], non dovrebbe sorprendere che l'*occasio* per avviare una ricerca sul tema delle possibili interazioni tra i *social network* e il sistema di giustizia penale muova da una considerazione empirico-statistica, prima ancora che scientifico-dogmatica. Si allude, in particolare, alla circostanza per cui le moderne piattaforme di *data sharing* (*Facebook*, *Instagram*, *Whatsapp*, *Telegram*, *Snapchat*, *TikTok*, etc.) pervadono ormai la vita di miliardi di persone in ogni parte del globo. Nessuno, allo stato attuale, può fondatamente dubitare dell'importanza assunta da questi "luoghi di interazione virtuale" nello svolgimento delle più varie ed eterogenee attività umane della quotidianità. Da semplici strumenti di comunicazione, i *social network* si sono rapidamente trasformati in veri e propri artefatti di "vita sociale", consentendo a ciascun individuo di plasmare la propria identità personale (analogica e digitale), nonché di instaurare o mantenere (pure a distanza) le proprie relazioni.

Preso atto, dunque, di questa estrema e capillare diffusività, è parso opportuno interrogarsi sull'*an* e il *quomodo* di eventuali implicazioni sul sistema di giustizia penale connesse all'impiego "in massa" e "di massa" di dette piattaforme. Del resto, l'idea di approfondire tale legame non dovrebbe apparire poi così peregrina laddove si consideri che il rito criminale, come autorevolmente osservato, riflette e si adatta allo «stato culturale dei popoli»[2]. Per di più, nell'ambito della giustizia penale – a differenza di quanto è dato riscontrare in altre branche del diritto[3] – risultano attualmente inesplorati, quantomeno a livello sistematico, i riflessi normativi di questo nuovo fenomeno digitale e "antropologico".

Ad ulteriore conferma della necessità di approntare uno studio organico della tematica, vi è, inoltre, un dato – che merita di essere sottolineato – proveniente dall'esperienza didattica sviluppatasi in numerose Università nordamericane. Navigando sul *web*, è possibile reperire programmi di insegnamento relativi a percorsi di Laurea in Giurisprudenza che offrono ai propri studenti la possibilità di approfondire le connessioni tra i *social network* e il sistema legale statunitense: possono di essere ricordati, ad esempio, gli insegnamenti di "*Social Media and Criminal Law*" e "*Social Media Law*" attivati presso l'Università di Dayton[4]. Un tanto testimonia il crescente interesse, a livello globale, per l'affermarsi di questa nuova "disciplina giuridica".

---

[1] M. CAPPELLETTI, *Dimensioni della giustizia nelle società contemporanee*, Bologna, 1994, p. 22.

[2] G. SABATINI, *Principi di diritto processuale penale*, vol. I, Catania, 1948, p. 38. Del resto, il diritto processuale penale ha natura "epifenomenica", cioè, «è il frutto delle meditazioni dei filosofi, delle teorie, delle scuole e, soprattutto, del costume di civiltà di un determinato popolo» (G. BELLAVISTA, *Studi sul processo penale*, vol. II, Milano, 1960, p. 216).

[3] Cfr. Parte I, Cap. II, par. 2.

[4] *https://udayton.edu/law/registrar/course_descriptions.php*. Già nell'anno 2017, si contavano 26 Università americane che includevano nei loro programmi di Laurea in Giurisprudenza corsi focalizzati sui *social media* e sul loro impatto nel settore legale (v. T.A. HOFFMEISTER, *Liking the Social Media Revolution*, in *Science and Technology Law Review*, 2017, p. 507, nt. 2).

Se quelle sommariamente accennate sono, dunque, le principali ragioni dello studio che si intende condurre, l'elaborato, dal punto di vista strutturale, si compone di tre parti.

Quanto alla prima (Parte I), la trattazione muove da una succinta analisi dell'impatto di *Internet* sull'ordinamento giuridico, in generale, e sul sistema di giustizia penale, in particolare (Capitolo I), per poi soffermarsi, più in dettaglio, sulla categoria centrale oggetto dello studio: i *social network sites* (Capitolo II). Poiché vi è la pregiudiziale esigenza di rintracciare l'origine e conoscere il concreto funzionamento dei sistemi di comunicazione (e di relazione) a mezzo *Internet*, le premesse dell'elaborato devono essere identificate proprio nell'esame della "storia della Rete". *Conditio sine qua non* per comprendere l'impatto giuridico di questo nuovo fenomeno "disruptivo"[5], il segmento iniziale della ricerca consentirà di mettere in luce, altresì, i diversi approcci che possono essere adottati dal giurista (e, in specie, dal processualista) per esplorare i fenomeni *online*.

Alla luce delle proposte coordinate teoriche, l'analisi prosegue esaminando le possibili implicazioni penal-procedimentali legate all'utilizzo delle *social-webpages* (Cap. III).

Sotto tale profilo, si avrà modo di osservare come una posizione di assoluto rilievo – tale da costituire il nucleo centrale, ancorché non esclusivo[6], dello studio – è rappresentata dal ricorso, sempre più massiccio, a strumenti informatico-digitali per finalità *lato sensu* investigative (Cap. III, par. 1 e 4); con ciò alludendosi a tutte quelle operazioni realizzate tanto nelle fasi di *intelligence* e di prevenzione criminale, quanto nello stadio più propriamente procedimentale. In questa prospettiva, si cercherà di far emergere come i *social network* costituiscano la più grande banca dati al mondo e, di riflesso, una vera e propria "miniera d'oro" di *bit* digitali. È per tale ragione, dunque, che l'immensa quantità di risorse *ivi* presenti – come si osserverà – sta ingenerando, sul versante procedimentale, una vera e propria metamorfosi dell'"istruttoria preliminare"; una fase che, oggi più di ieri, è chiamata a fare i conti con l'avvento di "tecniche investigative 2.0", il cui tratto distintivo risiede nella raccolta e nell'aggregazione massiva di informazioni.

Così individuata l'area tematica più complessa nei rapporti tra *social network* e giustizia penale, la seconda parte del lavoro (Parte II) sarà dedicata proprio allo studio delle diverse modalità di apprensione, a fini investigativi, del materiale informatico ricavabile dagli "spazi sociali virtuali".

A tal fine, è sembrato opportuno – tanto a livello logico, quanto metodologico – esaminare separatamente l'impiego di tali strumenti a seconda della tipologia o, meglio, dell'accessibilità dei dati oggetto di acquisizione (Cap. II, par. 1). La natura pubblica (Cap.

---

[5] Il riferimento corre alle cd. *Disruptive Technologies*. L'espressione, come noto, nasce con l'obiettivo di descrivere tutte quelle innovazioni capaci di rivoluzionare un precedente modello di *business*, stravolgendo il modo in cui i consumatori e gli utenti sono abituati a utilizzare determinati beni o servizi. In una prospettiva più generale, però, l'icastica locuzione è oggigiorno utilizzata – anche nel settore giuridico – per rappresentare un progresso e un'evoluzione della *technè* che si qualifica in termini non graduali, ma, per l'appunto, repentini, dirompenti e "distruttivi". Il termine *digital disruption* – che si inscrive nell'ambito delle numerose innovazioni apportate dalla cd. quarta rivoluzione industriale – allude, infatti, a un mutamento capace di generare nuovi paradigmi comunicativi, tecnologici e valoriali con specifico riguardo, ad esempio, alla robotica, all'intelligenza artificiale e ai *social network*. In proposito, v., *amplius*, T. ARMENTA DEU, *Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambio*, Madrid, 2021, p. 217 ss.

[6] Cfr. Parte I, Cap. III, parr. 2 e 3.

II e III), ristretta (Cap. IV) o segreta/riservata (Cap. V) delle informazioni presenti nelle *web communities*, difatti, impone di confrontarsi con mezzi di ricerca della prova talvolta del tutto inediti (come, ad esempio, il *social network patrolling* o la *false friends technique*), talaltra più tradizionali, ma le cui caratteristiche fisiologiche sono destinate a mutare dinnanzi al *bit* digitale.

Nell'ultima parte dell'elaborato (Parte III), infine, saranno presi in considerazione i risvolti *stricto sensu* processuali legati all'uso dei *social network sites* nella fase dibattimentale.

Sotto tale profilo, lo sguardo oltre i confini nazionali e il ricorso alle metodologie di indagine proprie dell'analisi comparata consentirà di mettere in luce i problemi con i quali i legislatori e le Corti di tutto il mondo, al netto della diversa tradizione giuridica di appartenenza (*civil law* o *common law*), sono chiamati a confrontarsi pressoché quotidianamente (Cap. I).

Al riguardo, appare sin da ora opportuno sottolineare come una particolare attenzione sarà dedicata allo studio dell'ordinamento e della giurisprudenza statunitense. Un approfondimento in tal senso offre un quadro davvero prezioso per comprendere come un sistema giuridico, notoriamente all'avanguardia nelle questioni legate all'impiego delle nuove metodologie di indagine digitale (specialmente in rapporto alle tensioni con il diritto alla *privacy*), stia affrontando la crescente presenza della "prova *social*" nel processo penale. L'esame di alcuni approcci esegetici, marcatamente innovativi, adottati dai tribunali nordamericani con riguardo al tenore letterale delle (alquanto generiche ed elastiche) *Federal Rules*, infatti, consentono di trarre insegnamenti utili a sviluppare strategie più efficaci, dal punto di vista normativo, per regolamentare l'impatto della *social network evidence* nel rito penale italiano.

In aggiunta, saranno analizzati anche alcuni aspetti del sistema processuale spagnolo (tanto a livello normativo, quanto giurisprudenziale). Con l'approvazione della *Ley organica* 5 ottobre 2015, n. 13, il legislatore iberico, mosso dalla necessità di adeguare le disposizioni del codice di procedura al progresso tecnologico, ha dettato una disciplina generale in tema di investigazioni penali informatiche. Guardata con le lenti del processualpenalista italiano, la regolamentazione in parola rappresenta senz'altro un modello di prim'ordine cui prendere spunto per una compiuta sistematizzazione della materia, giacché contiene riferimenti espliciti a principi che fungono da limite all'esercizio dello *ius investigandi*.

Se è vero, del resto, che i *social network* hanno già varcato la soglia delle aule di giustizia, il legislatore e la giurisprudenza nostrani non sembrano esserne ancora pienamente consapevole (Cap. II). Per tale ragione, si cercherà di riflettere sulle possibili soluzioni utili a garantire che l'ingresso della *social network evidence* nella fase dibattimentale avvenga nel pieno rispetto delle Regole del modello accusatorio, alle quali pure detta "tipologia probatoria 2.0" deve conformarsi.

PARTE I

SOCIETÀ, DIRITTO E NUOVI "CODICI COMUNICATIVI"

PROFILI GENERALI

CAPITOLO I

RELAZIONI UMANE DIGITALI E DISCIPLINE GIURIDICHE

SOMMARIO: 1. L'incidenza della tecnologia digitale nei rapporti sociali. – 2. Nascita ed evoluzione della "rete delle reti": dal *web* 1.0 alla cd. *Internet of Things*. Profili di interesse per l'indagine. – 3. Politiche legislative cibernetiche: i differenti approcci alla regolamentazione dei fenomeni giuridici *online*. – 4. I riflessi di *Internet* sul sistema penale. Cenni all'elaborazione dottrinale statunitense: *internal vs external perspective*. – 5. Dai "reati informatici" ai "reati cibernetici": *old wine in new bottles*? – 6. I risvolti processuali delle "connessioni di Rete": l'informatizzazione dell'apparato giudiziario e le nuove investigazioni penali digitali

1. L'incidenza della tecnologia digitale nei rapporti sociali

Un lavoro che, come esplicitato nel titolo, ambisce a fornire una ricostruzione critica delle potenziali connessioni tra le piattaforme di *sharing* (i cd. *social network sites*) e il sistema di giustizia penale, deve necessariamente muovere da alcune considerazioni introduttive, basate su un approccio di tipo sociologico e in una prospettiva improntata alle nuove Tecnologie dell'Informazione e della Comunicazione (ICT)[1]. Benché dette (brevi) riflessioni possano apparire, a prima vista, del tutto fuor d'opera rispetto a uno studio dedicato alla procedura penale, esse, come si cercherà di dimostrare nel corso della trattazione, risultano imprescindibili per cogliere appieno il cambiamento del *modus vivendi* delle persone nell'attuale "realtà digitale". È solo muovendo da tali premesse, difatti, che possono essere apprezzate affondo le implicazioni sul versante *lato sensu* processuale.

Si muova, dunque, dal principio.

La teoretica aristotelica, com'è noto, descrive l'essere umano alla stregua di un «animale sociale»[2] che tende ad aggregarsi con altri individui e a costituirsi in società, con il precipuo scopo di realizzare la sua più intima natura: lo sviluppo e l'esercizio della personalità e della Ragione. Il termine greco *πολιτικόν*, in questa visione, spiega e riassume assai efficacemente uno dei caratteri essenziali dell'uomo, ovverosia la sua "politicità", intesa come bisogno di confronto e di rapporto costante con i suoi simili, senza il quale egli si ridurrebbe a un essere solitario.

Nel perseguire tale obiettivo, l'individuo, fin dall'avvento delle prime «culture ad oralità primaria»[3] – nelle quali la comunicazione era essenzialmente basata su una trasmissione della conoscenza attraverso il suono –, ha sentito la necessità di ricorrere a specifici strumenti – quali i gesti, le immagini, la parola, la scrittura, la stampa e, da ultimo, gli artefatti elettronici – in grado di veicolare la rappresentazione del pensiero. A tal proposito, è agevole constatare come l'avanzamento della *téchne* abbia da sempre costituito il motore per l'avvento di nuove e sempre più sofisticate modalità comunicative: il passaggio dall'oralità

[1] Su tale concetto, anche per i riflessi sul piano giuridico, v., per tutti, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 9 ss.

[2] ARISTOTELE, *Politica*, Bari, 2007, par. 1253.

[3] L'espressione si deve a uno dei più autorevoli studiosi americani di antropologia e storia della comunicazione: W.J. ONG, *Oralità e scrittura. Le tecnologie della parola*, Bologna, 1986, p. 34.

alla scrittura, solo per fare un esempio, ha contribuito a modificare le capacità relazionali degli esseri umani, consentendo una più ampia diffusione delle idee e, con esse, della cultura (o, meglio, delle culture), nonché trasformando direttamente o indirettamente i «processi mentali»[4].

Se tali osservazioni possono ritenersi valide con riguardo alle grandi rivoluzioni comunicative del passato[5], considerazioni a parte merita, invece, il fenomeno dell'innovazione tecnologico-digitale al quale stiamo assistendo negli ultimi anni. Com'è stato efficacemente messo in luce, questo «si è instaurat[o] tra le maglie della società intera fino a liquefarsi nelle *routine* quotidiane di milioni di persone»[6], tanto da far sembrare inappropriato il ricorso al termine "tecnologia" per descrivere un fenomeno che, a ben riflettere, è stato ormai profondamente interiorizzato dalla maggior parte degli esseri umani[7].

In tale contesto, alcuni autori hanno osservato come la "digitalizzazione della società", quale causa primaria degli attuali mutamenti sociologici[8], avrebbe provocato un completo «assoggettamento di tutte le forme della vita culturale alla sovranità della tecnica e della tecnologia»[9]. A questa tesi – che assume il progresso quale «primo motore dei processi sociali»[10] – si contrappone una differente esegesi, in base alla quale il rapporto tra tecnologia e società non andrebbe impostato in termini meramente causali e, cioè, limitandosi ad osservare gli effetti prodotti dall'evoluzione digitale sulle scelte relazionali degli individui. Numerosi studi, infatti, dimostrerebbero come la stessa tecnologia venga plasmata dal contesto economico e culturale nel quale è chiamata a operare, nel solco di un'idea per cui «ogni progresso tecnico [viene] accompagnato, seguito e [spesso] preceduto dalle necessarie trasformazioni psicosociali»[11].

A prescindere da tale dibattito (comunemente ricondotto allo "scontro ideologico" tra il determinismo tecnologico e il determinismo sociologico), un dato appare incontrovertibile: la tecnologia digitale ha profondamente mutato il modo di concepire e intrattenere le relazioni tra gli esseri umani. Che la causa di tale cambiamento sia da ricondurre

---

[4] Così, nuovamente, W.J. ONG, *Oralità e scrittura*, cit., p. 119.

[5] Ci si riferisce, in particolare, al passaggio dall'oralità alla scrittura e dalla scrittura alla stampa.

[6] M. VERGANI, *L'impatto della tecnologia digitale sulla sociologia visuale: opportunità e sfide*, in *Studi di Sociologia*, 2009, p. 491.

[7] Mutuando, in tal modo, il paragone proposto, ancora una volta, da W.J. ONG, *Oralità e scrittura*, cit., p. 123, il quale mette in luce come la scrittura sia stata ormai interiorizzata così profondamente che pare difficile concepirla come una vera e propria forma di "tecnologia".

[8] Cfr. S. FABBRINI, *Nuove tecnologie, potere e cambiamento sociale*, in *Studi di Sociologia*, 1984, p. 135 ss.

[9] Per detta visione, v. N. POSTMAN, Technopoly. *La resa della cultura alla tecnologia*, Torino, 1993, p. 53. I comportamenti dell'uomo, secondo questa corrente di pensiero, sarebbero indotti e governati dal progresso delle scienze digitali che, muovendo da un'idea "deterministica" della tecnologia, finirebbero per attribuire all'individuo il ruolo di mero partecipe passivo dell'inarrestabile evoluzione informatica (M. FASOLI, *Contro lo strumentalismo tecnologico. Per una teoria analitica della prescrittività degli artefatti*, in *Sistemi intelligenti*, 2020, p. 223).

[10] M. DE BENEDITTIS, *Per una riconcettualizzazione del rapporto tecnologia/società*, in *Studi di Sociologia*, 2001, p. 318.

[11] L. MUMFORD, *II mito della macchina*, Milano, 1969, p. 231. La linea interpretativa in esame si inserisce nel solco di quel filone esegetico che qualifica gli strumenti tecnologici come semplici "mezzi", come tali, neutri. L'idea che la tecnologia, di per sé, non sia né buona, né cattiva e che tutto dipenda dall'utilizzo che di essa viene fatto, d'altro canto, è stata efficacemente ricondotta proprio a una «visione tecnologica del buonsenso» (così, M. FASOLI, *Contro lo strumentalismo tecnologico*, cit., p. 223).

esclusivamente al progresso delle scienze informatiche ovvero, prima ancora e/o contestualmente, a un'evoluzione del modo in cui i cittadini sono portati a concepire i rapporti umani importa fino a un certo punto: occorre prendere atto di tale trasfigurazione sociale. Le moderne tecnologie, a ben riflettere, non hanno semplicemente modificato il modo di comunicare, ma, riprendendo le parole di uno tra i più autorevoli filosofi del XXI secolo, hanno creato e forgiato «la nostra realtà fisica e intellettuale […] cambian[do] il modo in cui ci relazioniamo con gli altri e con noi stessi […], e [hanno fatto] tutto ciò in maniera pervasiva, profonda e incessante»[12].

2. Nascita ed evoluzione della "rete delle reti": dal *web* 1.0 alla cd. *Internet of Things*. Profili di interesse per l'indagine

In ragione di quanto osservato, la prima tappa del percorso che si vuole intraprendere deve muovere imprescindibilmente dalla comprensione delle conseguenze derivanti dell'impiego di tecnologie digitali sul modo di concepire, costruire e vivere i rapporti interpersonali.

Adottando questa prospettiva, l'analisi non può che prendere l'abbrivio dalla comparsa di *Internet*, uno strumento che, sul finire degli anni '60 del secolo scorso, ha dato vita a una vera e propria "realtà virtuale", liquida, diffusa e foriera di incertezze, ma, allo stesso tempo, fonte di indiscutibili opportunità. Espressione di un passaggio evolutivo di portata epocale, l'avvento della "rete delle reti"[13] incarna a pieno i connotati di quella che è stata definita la cd. quarta rivoluzione industriale[14], manifestazione di una nuova fase della storia umana caratterizzata da un mutamento profondo e sistemico della realtà socioeconomica.

Benché una compiuta rassegna storiografica della comparsa di *Internet* esuli dal presente lavoro, è comunque necessario dare succintamente conto dei momenti più significativi che hanno segnato il definitivo affermarsi della Rete. Ciò, in particolare, al fine di dimostrare come alcune categorie giuridiche ed elaborazioni dottrinali sviluppatesi in un determinato contesto sociale, ovverosia quello "pre-digitale", si rivelino talvolta inadeguate per affrontare le numerose sfide poste dalla "*New Age* informatica".

Dal punto di vista storico, la nascita di *Internet* è comunemente fissata nel 1969, anno in cui un gruppo di ingegneri e informatici americani, sovvenzionati dal Dipartimento di Difesa statunitense, elaborarono un programma militare, il cd. ARPANET (*Advanced Research Project Agency Network*), il cui obiettivo, nel clima esasperato della Guerra Fredda, era quello di assicurare il controllo e la tutela del sistema di comunicazione nordamericano a fronte di possibili attacchi provenienti dall'*ex* Unione sovietica.

Nel tortuoso percorso evolutivo che ha caratterizzato la storia della Rete[15], il punto di svolta – per quel che interessa in questa sede – si ebbe nel 1993, anno in cui alcuni ricercatori del CERN di Ginevra resero accessibile al grande pubblico un sistema di gestione di

[12] Testualmente, L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, IX.

[13] Così definita in ragione del suo funzionamento, basato, a differenza delle comuni reti informatiche, sulla relazione a livello globale di molteplici nodi periferici.

[14] L. FLORIDI, *La quarta rivoluzione*, cit., p. 1.

[15] In generale, sulla nascita ed evoluzione di *Internet*, cfr., per un affresco in lingua italiana, K. HAFNER – M. LYON, *La storia del futuro – Le origini di* Internet, Milano, 1998.

informazioni (denominato *Word Wide Web*) che, sfruttando le interconnessioni generate dai "cavi in rame", consentiva agli internauti di navigare in *Internet*, usufruendo di una grande quantità di servizi grazie all'innovativo sistema di collegamento ipertestuale, il cd. *link*. In tale contesto, la nascita del *web* di prima generazione («*web* 1.0»[16]) rispondeva appieno alle esigenze dell'*Homo Technologicus* (o *Homo Numericus*), ovverosia la possibilità di condividere informazioni e accedere a risorse da remoto. L'avvento di una «comunicazione internettiana»[17], infatti, costituisce il portato principale di *Internet*; da quel momento, chiunque e da qualunque luogo sarebbe stato in grado di connettersi con altri utenti, come in una grande "piazza virtuale".

Se, però, i primi modelli di elaboratori elettronici si limitavano a offrire ai propri utenti la mera possibilità di scambiare interazioni *one to one* o *one to many*[18] – senza consentire, invece, un vero e proprio "dialogo virtuale" –, è solo con il successivo sviluppo di piattaforme digitali in grado di far connettere tra loro un numero indeterminato di persone che si è potuto superare «l'originaria architettura "unidirezionale" del *web*, in cui l'utente era il destinatario passivo di informazioni e comunicazioni»[19].

L'emersione di una diffusa e pervasiva esigenza di interazione sociale, legata alla necessità di creare e condividere contenuti, ha portato alla comparsa di un nuovo mondo virtuale (cd. *web* 2.0), governato da flussi di trasmissione "intrinsecamente partecipativi". Sono nati, così, i primi *blog*, i *forum* e i sistemi di comunicazione in tempo reale (cd. *chat*), strumenti che consentono ai singoli fruitori del servizio di entrare in relazionale con terzi in via diretta, esprimendo opinioni o condividendo informazioni.

Il passaggio dal *web* 1.0. al *web* 2.0[20], come agevole constatare, non ha comportato solo una rivoluzione dal punto di vista tecnologico-digitale, ma, altresì, un radicale mutamento dei comportamenti umani e, di conseguenza, dei rapporti sociali, tanto che il ventaglio delle attività compiute "nella Rete" è ormai divenuto talmente ampio che, sotto certi aspetti, non appare più ragionevole distinguere tra "mondo fisico" e "realtà virtuale". Lo dimostrano, incontrovertibilmente, le statistiche più recenti relative all'utilizzo di *Internet*: nel gennaio 2023, circa il 66% della popolazione mondiale aveva accesso a un sistema di connessione *online* (5,16 miliardi utenti)[21]. Un dato che, a ben pensare, non stupisce affatto. D'altro canto,

---

[16] La paternità di tali espressioni è attribuibile a T. O'REILLY, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, in *Communications & Strategies*, 2007, 1, p. 17 ss. e, in part., p. 19, ove si individua in *Google* «*the standard bearer for Web 2.0*».

[17] Così la definisce P. COSTANZO, *Aspetti evolutivi del regime giuridico di* Internet, in *Dir. inf. e informatica*, 1996, p. 831.

[18] Si pensi ai primi sevizi *e-mail* o *fax*.

[19] L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 57.

[20] Secondo L. PICOTTI, *Diritto penale e tecnologie informatiche*, cit., p. 58, sarebbero ravvisabili due ulteriori forme di *web*. Attualmente, infatti, ci troveremmo nell'era del cd. *web* 3.0, un sistema di interconnessione di dati caratterizzato dalla multimedialità delle comunicazioni, ovverosia dalla possibilità di scambiare *file* audio, video e immagini attraverso dispositivi mobili. Ad avviso dell'A., inoltre, sarebbe prefigurabile, in un futuro non troppo remoto, l'avvento di una nuova forma di *web* 4.0 governata dai sistemi di intelligenza artificiale. Differente è, invece, la prospettiva adottata da S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, p. 322, che ricollega il *web* 3.0 all'avvento del cd. *Internet* delle cose (cfr. *infra*).

[21] *https://wearesocial.com/it/blog/2023/01/digital-2023-i-dati-globali/*.

specie nel mondo occidentale, l'utilizzo di una rete *wifi* è ormai divenuto essenziale e indispensabile per il compimento della maggior parte delle attività umane.

La straordinaria diffusione di *Internet*, in realtà, appare strettamente correlata a un altro fenomeno altrettanto travolgente (e coinvolgente) che, in qualche modo, costituisce un'evoluzione della "rete delle reti": il cd. *Internet of Things* (IoT)[22]. La locuzione, utilizzata per la prima volta nel 1999 dal britannico Kevin Ashton, descrive un sistema nel quale gli oggetti di uso comune (*smartphone*, autoveicoli, elettrodomestici, etc.) sono collegati a *Internet* tramite sensori che consentono un utilizzo (e un controllo) continuativo di tali dispositivi, offrendo così un contributo significativo per lo sviluppo della cd. società iperconnessa[23]. Se *Internet* "è in ogni cosa" (*rectius*, in ogni oggetto di uso quotidiano), ciò significa che qualunque attività umana, compiuta *online* od *offline*, è destinata a lasciare una "traccia digitale" che, elaborata congiuntamente ad altre informazioni, consente di ricostruire le vicende della vita e i pensieri più intimi di un individuo.

La breve e rapsodica descrizione dei principali momenti che hanno caratterizzato l'evoluzione di *Internet* consente di mettere in luce due aspetti prodromici per l'analisi che si intende condurre.

Il primo.

La storia del *web* può essere letta non solo in termini di "evoluzionismo tecnologico", ma anche come la cronaca di un progressivo sviluppo del modo di comunicare che, ad oggi, sembra non poter prescindere dall'utilizzo di artefatti digitali (*smartphone*, *tablet*, etc.). Un *modus comunicandi* che, è bene precisarlo, ha assunto una natura bidirezionale: uomo-macchina e macchina-uomo. Quando le persone confidano i loro pensieri a un assistente domotico come *Alexa* o quando navigano su *Firefox* alla ricerca di un buon ristorante non stanno facendo altro se non comunicare con un insieme di reti tra loro interconnesse.

Tutto ciò, sul versante giuridico, induce a riflettere sull'opportunità di predisporre regolamentazioni *ad hoc* in grado di cogliere a pieno questa evoluzione comunicativa. Dal punto di vista squisitamente processuale, il riferimento corre, ad esempio, alla possibilità di utilizzare a fini probatori le informazioni generate da tali sistemi. Di qui l'interrogativo se gli scambi di pensiero uomo-macchina possano o meno rientrare nel campo di applicazione dell'art. 15 Cost., volto a tutelare «ogni […] forma di comunicazione» e, dunque, se essi, ad esempio, possano formare oggetto di intercettazione. La genericità dell'espressione utilizzata dai Padri costituenti e la necessità di adattare la Carta delle Leggi alle nuove sfide della realtà tecnologica, lo si vedrà più approfonditamente, sembrerebbero legittimare

[22] Per un approfondimento sulla nascita e lo sviluppo di tale fenomeno, nonché per le sue implicazioni sul piano giuridico, v., di recente, L. DENARDIS, Internet *in ogni cosa. Libertà, sicurezza e* privacy *nell'era degli oggetti iperconnessi*, Roma, 2022.

[23] Già nel 2009 la Commissione europea aveva messo in luce come «l'*Internet* degli oggetti non deve essere considerato un concetto utopistico» poiché «diverse applicazioni pionieristiche dell'*internet* degli oggetti sono già in fase applicativa» (COMMISSIONE EUROPEA, *L'*Internet *degli oggetti – Un piano d'azione per l'Europa*, 18 giugno 2009, p. 3).

un'interpretazione evolutiva di tale concetto[24], fino a ricomprendervi qualunque tipologia di *digital communication* e, pertanto, anche le interazioni *human-computer*[25].

Il secondo.

Gli strumenti digitali di uso quotidiano hanno acquisito la straordinaria capacità di immagazzinare un numero elevatissimo di informazioni, il cui trattamento mediante sofisticati algoritmi consente di ricostruire "a tavolino" la vita di un individuo: spostamenti, relazioni interpersonali, emozioni e financo i propri desideri più intimi. Semplici gesti come la ricerca di un indirizzo su *Google Maps*, la scelta di una canzone su *Amazon Music* o il "postare"[26] un video su *TikTok* possono essere letti e analizzati per studiare il comportamento degli esseri umani[27]. Senza rendersene conto, gli individui hanno iniziato a confidare i loro segreti, anche quelli inconfessabili, a macchine intelligenti in grado di conservarli, gestirli e utilizzarli per finalità che spesso sfuggono al loro controllo. I dati immagazzinati nel *web*, allo stato attuale, consentono ai gestori delle piattaforme (e non solo) di penetrare nella sfera più intima e riservata dell'uomo: è in gioco la tutela dei dati personali dei cittadini e la salvaguardia della legittima riservatezza della loro vita privata.

In un contesto, dunque, nel quale le informazioni, come sovente osservato, costituiscono il "petrolio del terzo millennio", compito del giurista, sotto tale secondo profilo, dev'essere quello di interrogarsi in merito alla gestione, all'utilizzo e alla tutela di tutti quei dati generati, più o meno consapevolmente, dagli utenti della Rete.

3. Politiche legislative cibernetiche: i differenti approcci alla regolamentazione dei fenomeni giuridici *online*

Come ogni ambito del sapere, anche la scienza giuridica si è dovuta confrontare con le numerose e complesse innovazioni apportate dalla "società digitale"[28]: «*ubi societas technologica, ibi ius*»[29]. Se il diritto è, anzitutto e prima di tutto, entità regolatrice dei rapporti sociali, e la tecnologia informatica, come si è visto[30], ha profondamento inciso sul *modus comunicandi* dell'uomo– nonché sulla struttura delle sue relazioni interpersonali –, la legge deve prendere atto di tali cambiamenti, al fine di predisporre un'adeguata regolamentazione della realtà circostante.

In tale contesto, gli studiosi, al cospetto di un «diritto artificiale»[31], devono farsi carico della trasformazione sociale in atto, al fine di valutarne i riflessi sul piano *stricto sensu* giuridico, nella consapevolezza che tale operazione dev'essere compiuta in un'epoca nella

---

[24] Cfr. Parte II, Cap. I.

[25] Sulla necessità di estendere il concetto di comunicazione anche alle «*machine-to-machine interaction or human-computer interaction*», v. S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020, p. 59 s.

[26] Trattasi di un neologismo, accreditato dall'Enciclopedia Treccani nell'anno 2013, con il quale si intende descrivere l'attività di «inviare un *post* in *Internet*», come, ad esempio, attraverso la condivisione di una foto su un *social network*.

[27] L. FLORIDI, *La quarta rivoluzione*, cit., p. 138.

[28] In proposito, cfr. l'opera pioneristica di V. FROSINI, *Cibernetica diritto e società*, Milano, 1968.

[29] T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. inf. e informatica*, 2020, p. 465.

[30] Cfr. *supra*, par. 1.

[31] Mutuando l'espressione utilizzata da V. FROSINI, *Cibernetica diritto e società*, cit., p. 12.

quale si assiste a un costante e giornaliero processo di metamorfosi della figura del «giurista come umanista in quella del giurista tecnologo»[32].

Si tratta, però, di un'operazione assai complessa. E questa difficoltà, a ben pensare, è dovuta alle caratteristiche intrinseche di *Internet*: transnazionalità, a-spazialità, libertà di accesso e anonimato. Il cyberspazio[33], infatti, è un luogo virtuale privo di frontiere, un'architettura acefala e decentralizzata nella quale ciascun cibernauta è libero di navigare alla ricerca delle innumerevoli risorse digitali messe a disposizione dalla Rete. La mediazione offerta da *Internet*, inoltre, consente all'utente di muoversi "senza essere visto": egli esprime la propria identità digitale godendo di una legittima pretesa di anonimato.

Questi connotati, sebbene costituiscano la ragione principale del successo della Rete nel panorama socioeconomico, hanno posto al centro della scena interrogativi giuridici di non poco momento.

Da un lato, non può negarsi come tali caratteristiche abbiano giocato un ruolo decisivo nello sviluppo e nell'esercizio di numerosi diritti fondamentali, incrementando così la percezione di libertà di ogni cittadino. Epperò, dall'altro, esse hanno incentivato forme innovative (e, non di rado, distorsive) di utilizzo del cyberspazio, rendendo così indispensabile la predisposizione di una disciplina *ad hoc* capace, se non di limitare l'accesso alla Rete, quantomeno di regolamentarlo.

È in tale contesto che si sono sviluppate le prime riflessioni in merito alla cd. *Internet Governance*, ossia al "se" e "come" disciplinare le attività umane *online*[34]. Non essendo necessario, ai fini dello studio, ripercorrere analiticamente il dibattito sorto sul punto, mette conto osservare come la strutturale ubiquità e trasversalità delle attività in Rete induca a censurare tanto quelle scelte interpretative volte ad attribuire, in via esclusiva, una *potestas*

[32] T.E. FROSINI, *Il diritto costituzionale di accesso ad* Internet, in M. Pietrangelo (a cura di), *Il diritto di accesso ad* Internet, Napoli, 2011, p. 23. In questo senso, vi è stato perfino chi ha ritenuto, provocatoriamente, che le moderne tecnologie impongano una «*capacidad programadora del jurista*» (E.C. PÉREZ-LUÑO ROBLEDO, *El procedimiento de Habeas Data. El derecho procesal ante las nuevas tecnologías*, Madrid, 2017, p. 38).

[33] Il termine *cyberspace* è stato utilizzato per la prima volta da William Gibson nel racconto *Burning Chrome* del 1982 per indicare una realtà virtuale generata dal *computer*. Etimologicamente, l'espressione *de qua* deriva a sua volta dal termine *Cybernetics*, coniato da Norbert Wiener, matematico americano che tra i primi nel panorama mondiale cominciò ad approfondire il fenomeno della cibernetica, definendo quest'ultima come «la scienza del controllo e della comunicazione negli animali e nelle macchine» (cfr. N. WIENER, *La cibernetica*, Milano, 1953, p. 3). Ancorché non possa individuarsi una definizione accettata a livello globale di tale locuzione, tra le nozioni maggiormente accreditate può farsi riferimento a quella offerta dal Dipartimento della Difesa degli Stati Uniti d'America: «*a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*» (DEPARTMENT OF DEFENSE, *Dictionary of Military and Associated Terms*, 8 November 2010, p. 58).

[34] Si rinvia, per tutti, alla panoramica, particolarmente accurata, offerta da L.A. BYGRAVE – L. BING, *Internet Governance: Infrastructure and Insitution*, Oxford, 2009.

normativa in capo agli Stati nazionali[35], quanto le esegesi dottrinali che ipotizzano una gestione affidata esclusivamente a soggetti e gruppi privati[36].

Appaiono, invece, maggiormente condivisibili quelle tesi che, sebbene con modulazioni eterogenee, individuano nella co-regolamentazione pubblico-privata, in una dimensione necessariamente sovranazionale, la forma più ragionevole per disciplinare giuridicamente le attività compiute in Rete[37].

Volendo percorrere quest'ultimo tracciato, il problema con il quale occorre confrontarsi concerne il *quomodo*. Come regolamentare dette attività? Tradizionalmente, il dibattito è stato ricondotto alla dicotomia tra *exceptionalists* e *unexceptionalists*[38].

I primi, come noto, sottolineano la necessità di adottare un approccio "innovativo", sostenendo che la nuova realtà digitale richiede uno sforzo del giurista per creare nuove categorie dogmatiche capaci di governare lo tsunami tecnologico. Ciò che accade in Rete, in altre parole, non potrebbe essere in alcun modo interpretato come una mera riproduzione di quanto accade nella realtà fenomenica, bensì costituirebbe – a detta di tali autori – una manifestazione "diversa e altra" di quelle attività compiute nel cd. *Virtual Word*.

Le tesi "non-eccezionaliste", per contro, muovono dall'idea che ogni operazione compiuta in Rete possa essere ricondotta, sfruttando un linguaggio metaforico[39], a un comportamento esteriormente percepibile; ogni condotta virtuale, detto altrimenti, avrebbe un proprio corrispettivo funzionale nella realtà materiale. Cosicché, il fenomeno *online* potrebbe essere agevolmente governato facendo ricorso all'applicazione di leggi già pensate, create e sviluppate per il mondo fisico.

A ben considerare, il brocardo di aristotelica memoria, *in medio virtus stat*, suggerisce di adottare una posizione mediana.

Per un verso, appare eccessivamente *tranchant* l'idea secondo la quale i fenomeni *online* possono essere governati ricorrendo esclusivamente alla creazione di nuove categorie giuridiche, sul presupposto di un'inadeguatezza dei principi e delle regole pensate per il mondo reale.

Per altro verso, risulta parimenti criticabile la scelta di inquadrare le nuove "fattispecie internettiane" nell'ambito di percorsi già battuti, specie mediante il ricorso a un linguaggio

---

[35] Una tale opzione avrebbe quale diretta (e irragionevole) conseguenza il contemporaneo assoggettamento delle attività compiute su *Internet* «*to the laws of all territorial sovereings*» (così, in senso giustamente critico, D.R. JOHNSON – D. POST, *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, p. 1374).

[36] Questa tesi è stata autorevolmente sostenuta da L. LESSING, *Code And Other Laws of Ciberspace*, New York, 1999, *passim*. La reiezione di tale esegesi si giustifica, tra l'altro, alla luce del fatto che, come si è già osservato, i naviganti del *web* utilizzano i servizi messi a disposizione dalla Rete per il compimento della maggior parte delle attività quotidiane, contribuendo così a creare un *database* di informazioni sensibili e ad alto contenuto conoscitivo, potenzialmente in grado di costituire il presupposto per una sorveglianza globale di massa gestita da *corporates* mosse da interessi puramente economici.

[37] In questo senso, v., ad esempio, I. BROWN – C.T. MARSDEN, *Regulating Code. Good Governance and Better Regulation in the Information Age*, Cambridge-Londra, 2013, *passim*.

[38] Cfr., per un affresco, J.L. GOLDSMITH, *Against Cyberanarchy*, in *University of Chicago Law Occasional Paper*, 1999, 40, p. 1199 ss.

[39] Si pensi a quelle espressioni che richiamano luoghi della realtà materiale (indirizzo di posta elettronica, localizzazione di risorse sul *web*; *homepage*, etc.) o a locuzioni che alludono a movimenti fisici (entrare nel sito *web*; navigare in Rete, etc.).

metaforico per descrivere ciò che accade nella Rete[40]. Ancorché risulti comprensibile l'utilizzo di similitudini per ricondurre a unità un fenomeno prima sconosciuto, un simile *modus operandi*, com'è stato acutamente osservato, non consente di apprezzare appieno le reali conseguenze giuridiche della tecnologia digitale[41]. Il paradigma informatico, infatti, produce di frequente, non solo un cambiamento nella modalità di realizzazione di un determinato evento, ma, talvolta, anche una «obsolescenza di contenuti essenziali di alcune tradizionali categorie dogmatiche»[42].

In conclusione, appare più ragionevole l'adozione di un approccio settoriale che faccia emergere, caso per caso, se il fenomeno oggetto di studio richieda un mero *upgrade* della regolamentazione vigente (ad esempio, ricorrendo a interpretazioni evolutive del dato normativo) o, al contrario, la necessità di predisporre un nuovo ordito legislativo, le cui fondamenta siano costituite da categorie giuridiche "*internet-oriented*".

4. I riflessi di *Internet* sul sistema penale. Cenni all'elaborazione dottrinale statunitense: *internal vs external perspective*

Com'era prevedibile, anche la scienza penale, al pari delle altre branche del diritto, è stata chiamata a confrontarsi con i riflessi giuridici di una società sempre più iper-connessa, schiudendo prospettive d'indagine affascinanti e, per certi aspetti, avveniristiche.

Prima di esaminarle più nel dettaglio, però, è opportuno muovere da una considerazione di carattere preliminare. Oggigiorno, la convinzione che si sta facendo strada tra un numero sempre più nutrito di studiosi è quella di abbandonare approcci squisitamente settoriali[43] che, troppo spesso, non consentono un'analisi efficace dei fenomeni con i quali il giurista moderno è chiamato a confrontarsi. In questo senso, è ricorrente imbattersi in analisi che mettono in luce lo stretto legame intercorrente tra il diritto penale sostanziale e il diritto penale processuale, ossia tra i "due mondi" della giustizia penale: il secondo non può sopravvivere in assenza del primo; ma, quest'ultimo, non può concretamente esplicare la sua funzione punitiva se non attraverso il processo[44].

Quanto detto, ancorché in una prospettiva di carattere generale, non può non assumere un qualche valore pure con riguardo al tema della "giustizia penale digitale": qui, più che altrove, appare necessario adottare un approccio di carattere unitario che valorizzi le interconnessioni tra profili sostanziali e processuali. Le peculiarità che contraddistinguono i crimini informatico-digitali, infatti, hanno fatto emergere la necessità di predisporre, su

---

[40] In tal senso, v. anche A. MORELLI – O. POLLICINO, *Le metafore della rete. Linguaggio figurato,* judicial frame *e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto*, in *Rivista AIC*, 2018, 1, p. 1 ss.

[41] G. FIORINELLI, Nomina nuda tenemus*? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche*, in *Discrimen*, 3 gennaio 2023, p. 8, per la quale «non deve sfuggire, tuttavia, che ogni metafora, pur essendo all'inizio un utile strumento per "liberare il pensiero", possa finire tuttavia per "soggiogarlo"».

[42] L. PICOTTI, *Diritto penale e tecnologie informatiche*, cit., p. 33.

[43] M. GIALUZ – J. DELLA TORRE, *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022, p. 290.

[44] Cfr. Parte II, Cap. I, par. 1. Onde rendersi conto di ciò, è sufficiente ricordare come illustre dottrina abbia efficacemente osservato che la «norma penale» non ha, in realtà, né una natura sostanziale, né processuale, bensì «reale», cioè, composta da elementi che, «per convenzione scolastica, vengono definiti di diritto sostanziale e di porzioni che vengono definite, sempre per ragioni espositive, di diritto processuale» (M. GALLO, *Diritto penale e Costituzione*, in *Dir. pen. cont.*, 25 ottobre 2018, p. 4).

entrambi i fronti, un *corpus* normativo *ad hoc* capace di rappresentare le diverse facce del fenomeno in parola. D'altro canto, il sistema penale tradizionale, così come le garanzie a esso sottese, sono stati pensati e modellati per prevenire, investigare, accertare e sanzionare una delinquenza "fisica" e "corporea", non certo per rispondere alle nuove sfide poste dall'era digitale.

Si è consapevoli, invero, come tale ultima affermazione non risulti unanimemente condivisa in letteratura. Come noto, infatti, la scelta dell'impostazione metodologica da adottare nello studio di ciò che avviene *online* è tutt'ora al centro di un acceso dibattito.

In un fondamentale saggio di inizio millennio, autorevole dottrina ha acutamente sottolineato come l'individuazione della regolamentazione giuridica più adeguata ad affrontare quanto accade nella Rete «*depend on facts, and the facts of the Internet depend on which perspective we choose*»[45].

Abbracciando una «*internal perspective of an Internet user*» (cd. *virtual point of view*) – si afferma – la legge applicabile ai fenomeni digitali è ricavata mediante il ricorso a similitudini e analogie tra il mondo reale e quello virtuale[46]. Privilegiando, invece, una «*external perspective*» (cd. *point of view of the physical world*), *Internet* si riduce a una mera rete di *computers* dislocati in tutto il mondo e connessi tra loro attraverso semplici cavi metallici; di talché «*the fact that Internet users may perceive that they have entered a virtual world of cyberspace has no particular relevance*»[47].

L'adozione di una prospettiva piuttosto che un'altra produce effetti tutt'altro che irrilevanti anche in campo processuale. Onde rendersi conto di ciò, è sufficiente richiamare il primo e noto caso di intercettazioni telefoniche nella storia della Corte Suprema degli Stati Uniti.

In *Olmstead*[48], la polizia giudiziaria, in assenza di un *placet* autorizzativo e al fine di smascherare un'imponente operazione di contrabbando, aveva sottoposto a captazione telefonica le comunicazioni tra l'imputato e alcuni suoi complici. La questione giuridica oggetto di causa può essere riassunta nei seguenti termini: la tutela della riservatezza apprestata dal quarto emendamento della Costituzione americana[49] può essere estesa al punto di includervi anche le comunicazioni intercorse tra due soggetti mediante cavi telefonici collocati sulla pubblica via?

La Corte, nel rispondere negativamente al quesito, aveva adottato, più o meno consapevolmente, un approccio di tipo "esterno": chi installa in casa propria uno strumento telefonico e intende proiettare la propria voce a chi si trova all'esterno, mediante l'utilizzo di cavi elettrici ubicati lungo le strade pubbliche, non può vantare alcuna pretesa di

---

[45] Così, assai efficacemente, O.S. KERR, *The Problem of Perspective in Internet Law*, in *Georgetown Law Journal*, 2003, p. 361.

[46] In tal senso, ad esempio, l'esperienza dell'utente del *web* che acquista un prodotto su *Amazon* può essere equiparata, tanto dal punto di vista fattuale, quanto giuridico, a quella di un cittadino che si reca in un "negozio fisico" per acquistare il medesimo bene.

[47] O.S. KERR, *The Problem of Perspective in Internet Law*, cit., p. 340.

[48] *Olmstead v. United States*, 136, 277 U.S. 438. (1928).

[49] «*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*».

riservatezza. Le voci captate – in questa prospettiva – corrono lungo fili elettrici che, data la loro collocazione, non possono essere considerati luoghi privati, così come non lo sono le strade lungo le quali gli stessi corrono. In assenza di un'invasione fisica nel proprio domicilio, dunque, nessuna ragionevole aspettativa di *privacy* poteva essere invocata dal ricorrente, di talché il IV Emendamento non avrebbe dovuto trovare applicazione.

Di diverso avviso era, invece, l'opinione dissenziente sostenuta del giudice Brandeis. Privilegiando quello che oggi si definirebbe "approccio interno", l'autorevole magistrato della Corte Suprema – Padre del moderno concetto di *privacy*[50] – ha sottolineato l'irrilevanza dell'ubicazione fisica dei fili elettrici ai fini dell'operatività della tutela garantita dal quarto emendamento. Ciò che avrebbe dovuto essere valorizzato, per contro, era la circostanza per cui qualora una linea telefonica venga sottoposta a captazione, la *privacy* dei colloquianti che si trovano alle sue estremità viene inesorabilmente "posta sotto assedio".

Il caso richiamato dimostra, con plastica evidenza, come l'adozione dell'uno o dell'altro approccio possa condurre a soluzioni interpretative collocate agli antipodi: il punto di osservazione del fenomeno digitale, dunque, influenza l'esegesi delle norme e, di riflesso, la loro concreta applicazione.

5. Dai "reati informatici" ai "reati cibernetici": *old wine in new bottles*?

È affermazione ricorrente quella per cui la traslazione della vita reale sugli schermi dei *computers* e degli *smartphones* – quale conseguenza dell'utilizzo massivo di *Internet* – abbia inevitabilmente comportato l'incremento del suo impiego anche per finalità illecite. La diffusione di artefatti comunicativi virtuali e, di conseguenza, l'aumento esponenziale delle occasioni di connessione e di condivisione in Rete pongono il problema della previsione normativa di fattispecie incriminatrici volte ad arginare il fenomeno della crescita esponenziale degli illeciti commessi dagli internauti.

Se queste sono le premesse, l'analisi che si va conducendo non può non soffermarsi, seppur brevemente, sull'avvento dei cd. *computer crimes*, ovverosia gli antenati nobili delle attuali forme di criminalità digitale, variamente definite ricorrendo a espressioni quali *cybercrime*, *e-crime* o *hi-tech crime*.

Ancorché la nascita di un'autonoma branca della scienza giuridica denominata "diritto penale dell'informatica"[51] venga sovente ricondotta agli inizi degli anni '60 – periodo nel quale i penalisti di tutto il mondo si sono confrontati, per la prima volta, con fattispecie di reato nelle quali il *computer* costituiva l'oggetto o lo strumento dell'azione criminosa[52] –, è solo con la diffusione delle "connessioni di rete" che si è iniziato a parlare di un vero e proprio "diritto penale dell'*Internet*"[53].

---

[50] S.D. WARREN – L.D. BRANDEIS, *The Right to Privacy*, in *Harward Law Review*, 1890, 4, p. 193 ss.

[51] Su tale categoria, cfr., per tutti, L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Id. (a cura di), *Il diritto penale dell'informatica nell'epoca di* Internet, Padova, 2004, p. 21 ss.

[52] *In primis*, D. PARKER, *Crime by Computer*, New York, 1976.

[53] D'altra parte, la dottrina più accreditata ha da tempo sottolineato la distinzione che intercorre tra i reati informatici e le diverse forme di criminalità nel cyberspazio: ciò che caratterizza l'utilizzo a fini illeciti della rete telematica «è la peculiarità che presenta il sistema di telecomunicazione» e, cioè, «un sistema che non ha una disciplina specifica ed universale; che non è comandato e controllato da alcuna autorità sovranazionale;

In realtà, non sfugge come qualunque operazione dogmatica diretta a un'*actio finium regundorum* tra queste macroaree appaia complessa.

La difficoltà di imbrigliare in aprioristiche categorie teoriche un fenomeno dalle manifestazioni tanto eterogenee emerge da una semplice analisi di tipo lessicale. A seguito del pioneristico studio di Parker – al quale si deve il merito di aver sviluppato una delle prime tassonomie sui *computer crimes*[54] –, la letteratura scientifica ha tentato di enucleare nuove formule per descrivere un *quid* difficilmente inquadrabile nelle tradizionali categorie giuridiche: si pensi, in questo senso, al ricorso a espressioni quali *digital crime* ed *electronic crime* che, pur muovendosi nella pregevole direzione di ricondurre a unità un macrocosmo all'evidenza ingovernabile, appaiono eccessivamente stringenti o già superate dall'evoluzione della tecnica.

Per tale ragione, la dottrina più accreditata ha prospettato, nell'ambito della categoria dei reati informatici, una duplice classificazione. In un primo gruppo dovrebbero essere ricondotti i cd. crimini informatici in senso stretto e, cioè, tutte quelle attività illecite che implicano una connessione «a procedimenti di elaborazione automatizzata di dati, secondo programmi informatici»[55]. In una seconda classe, invece, dovrebbero collocarsi tutte quelle ipotesi nelle quali la condotta criminosa può essere realizzata anche – ma non esclusivamente – per mezzo di apparecchiature informatiche (cd. reati informatici in senso ampio)[56].

Com'era prevedibile, però, le difficoltà ricostruttive nell'addivenire a una nozione condivisa di crimine informatico si sono manifestate nuovamente con riguardo al tema dei reati cibernetici. L'impostazione dominante tende a ricondurre in tale categoria tutti quegli illeciti caratterizzati dalla «diretta realizzazione o proiezione del fatto tipico»[57] nel *cyberspace*.

Anche in questo caso, in ragione dell'eterogeneità del fenomeno qui in esame, si è ritenuto opportuno distinguere due *species*. Da un lato, i reati cibernetici in senso proprio, ipotesi nelle quali la fattispecie incriminatrice contiene un espresso riferimento alla Rete o al *web* quale luogo di realizzazione della condotta[58]. Dall'altro, i *cybercrimes lato sensu* intesi, nei quali la realizzazione dell'attività criminosa può avvenire tanto "in Rete", quanto nel "mondo fisico"[59].

Il breve *excursus* consente di mettere in luce come le nuove potenzialità criminogene scatenate dalla diffusione di *Internet* abbiano indotto gli studiosi di diritto penale a interrogarsi sulla necessità di approntare nuovi modelli di tutela. A fronte di tesi

---

che consente agli utenti l'assoluto anonimato» (così, C. PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, p. 33).

[54] D. PARKER, *Crime by Computer*, cit., p. 20, il quale riconduce la categoria in parola a quelle ipotesi nelle quali il *computer* costituisce l'oggetto, lo strumento o il simbolo del crimine, nonché l'ambiente in cui esso viene realizzato.

[55] Così, L. PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. econ.*, 2011, p. 845. Si consideri l'ipotesi prevista all'art. 615-*ter* c.p., fattispecie nella quale il legislatore richiama testualmente espressioni riconducibili alla tecnologia informatica («sistema informatico o telematico protetto da misure di scurezza»).

[56] Come, ad esempio, il delitto di pornografia minorile (art. 600-*ter* c.p.).

[57] L. PICOTTI, *La nozione di «criminalità informatica»*, cit., p. 847.

[58] Si consideri, in via esemplificativa, il delitto di *cyberstalking* previsto all'art. 612-*bis* c.p.

[59] Si pensi al reato di diffamazione *online*.

irragionevolmente conservatrici[60] ed esegesi fideisticamente progressiste[61], l'impostazione che sembra prevalere, come spesso accade, può essere identificata in un *mix compositum* fra le due prospettazioni. A livello legislativo, ad esempio, ci si è limitati, talvolta, a realizzare un mero adeguamento delle fattispecie già esistenti, interpolando il tessuto normativo nei limiti dello stretto necessario, in ossequio al principio di *extrema ratio* che, se correttamente inteso, costituisce un canone direttivo teso a ridurre al minimo il ricorso allo strumento penale. In altri casi, invece, i Parlamenti nazionali hanno ritenuto opportuno muoversi verso la creazione di nuove e inedite ipotesi criminose che, alle volte, ricalcando la struttura di fattispecie già presenti nell'ordito codicistico, hanno però generato notevoli incertezze interpretative, «data la difficoltà di far rientrare fatti, condotte od oggetti profondamente diversi in schemi concepiti per realtà differenti»[62].

6. I risvolti processuali delle "connessioni di Rete": l'informatizzazione dell'apparato giudiziario e le nuove investigazioni penali digitali

In un saggio del 1998, autorevole dottrina si interrogava su quale impatto avrebbe potuto avere l'avvento di *Internet* sul processo penale italiano[63]. L'Autore, dopo aver messo in luce il duplice rapporto instauratosi tra *bit* digitali e rito criminale[64], concludeva sostanzialmente adottando un giudizio di *non liquet*: «è certo presto per fare un primo, anche solo provvisorio, bilancio dell'influenza che *Internet* è in grado di sviluppare sullo svolgimento delle procedure giudiziarie e, in particolare, di quelle penali. Nonostante se ne parli molto, tale strumento è finora accessibile a una cerchia limitata di persone»[65]. Quasi un anno dopo, la Corte statunitense per il distretto meridionale del Texas[66], chiamata a pronunciarsi nel merito di una causa avente ad oggetto l'infortunio subito da un impiegato nel corso della propria attività lavorativa, rigettava le pretese avanzate dal *plaintiff* – fondate, essenzialmente, su differenti tipologie di *electronic evidence* –, equiparando le notizie ricavate dal *web* a delle «*voodoo information*» e concludendo nel senso che «*any evidence procured off the Internet is adequate for almost nothing*».

Sebbene tali posizioni possano apparire oggigiorno anacronistiche, esse si collocano in un periodo storico nel quale, come già ricordato[67], il gruppo di ricerca del CERN di Ginevra aveva da poco reso accessibile al grande pubblico il *Word Wide Web*. Lo scetticismo

---

[60] In tale categoria può essere ricondotto il pensiero di coloro che consideravano i reati informatici come una semplice tipologia di crimine tradizionale, sebbene commesso con il ricorso a nuove strategie tecnologiche. Emblematica, in tal senso, l'espressione coniata dal criminologo e informatico Peter Grabosky, il quale, interrogandosi sulla natura dei nuovi "crimini digitali", si chiese se il *cybercrime* fosse «*old wine in new bottles or new wine*» (P.N. GRABOSKY, *Virtual Criminality: Old Wine in New Bottles?*, in *Social & Legal Studies*, 2001, p. 243 ss.).

[61] D. PETRINI, *La responsabilità penale per i reati via* Internet, Napoli, 2004, p. 59.

[62] Così si esprime L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 53.

[63] R. ORLANDI, *Il processo nell'era di* Internet, in *Dir. pen. proc*., 1998, p. 140.

[64] R. ORLANDI, *Il processo nell'era di* Internet, cit., p. 140: «conviene cioè esaminare distintamente l'"informazione" nel (o per il) processo – informazione intesa, cioè, come contenuto dell'accertamento penale e come fattore di conoscenza che rende possibile l'elaborazione di decisioni giudiziali – dalla "informazione" sul processo, vale a dire, quella che ha nell'attività processuale il proprio oggetto».

[65] Testualmente, ancora, R. ORLANDI, *Il processo nell'era di* Internet, cit., p. 140.

[66] *St. Clair v. Johnny's Oyster & Shrimp*, 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999).

[67] Cfr. *supra*, par. 2.

rappresentato dalle parole del tribunale federale americano e la cautela manifestata della dottrina italiana, dunque, apparivano – e appaiono tutt'oggi – senz'altro comprensibili, se non condivisibili.

A distanza di poco più di vent'anni, però, l'inarrestabile progresso tecnologico, «portante chiave di ogni modernità»[68], ha radicalmente mutato le condizioni di contesto e, di riflesso, l'approccio alla materia penal-processuale.

Muovendosi in una prospettiva ancora generale, costituisce affermazione ricorrente – nonché un dato di realtà agevolmente osservabile – quella per cui il rapporto tra la dimensione tecnologica e il procedimento penale connoti ormai l'incedere del rito in tutte le sue articolazioni, trovando terreno fertile nell'ambito del diritto delle prove, delle metodologie di investigazione, passando per la fase decisoria, fino a coinvolgere il concreto espletamento degli atti processuali. L'avvento di *Internet* ha inciso, perciò, su numerosi ambiti del procedimento penale, schiudendo prospettive di indagine che fino a pochi anni fa sarebbero state inimmaginabili o, quantomeno, avveniristiche.

Tra queste, il tema della cd. informatizzazione dell'apparato giudiziario e quello relativo alla cd. *digital evidence* (nonché, di riflesso, alla *digital investigation*) appaiono indubbiamente i più significativi[69].

Si considerino, sul primo versante, le nuove modalità di deposito, trasmissione, notificazione e comunicazione degli atti processuali. Grazie alle potenzialità di connessione alla Rete, l'avvento di un vero e proprio processo penale telematico non è più un miraggio, tanto affascinante quanto inafferrabile. Com'è noto, infatti, la previsione di specifici strumenti atti a consentire agli attori del processo – e ai comuni cittadini[70] – un'efficiente ed efficace interazione "a distanza" con la macchina giudiziaria è certamente una delle conquiste di maggior spessore della recente novella che ha interessato il sistema penale (cd. riforma Cartabia)[71].

Senz'altro più interessanti, ai fini della presente trattazione, si appalesano i numerosi (ed epocali) riflessi sul piano dell'"inchiesta penale". Quella stessa tecnologia della Rete inizialmente pensata per comunicare, partecipare, apprendere o, come detto, delinquere, ha cominciato a essere utilizzata come legittimo strumento di investigazione da parte delle forze di sicurezza pubblica. In proposito, la sociologia giudiziaria ci consegna l'immagine di una fase investigativa dai connotati profondamente alterati rispetto a quelli che i *conditores* le avevano attribuito al momento della redazione del "nuovo" codice. È fuor di dubbio, in effetti, come la ricerca degli elementi di prova – e, ancor prima, della stessa notizia di reato

[68] Riprendendo le parole di G. DI CHIARA, *Il canto delle sirene. Processo penale e modernità scientifico-tecnologica: prova dichiarativa e diagnostica della verità*, in *Criminalia*, 2007, p. 21.

[69] La circostanza è sottolineata, da ultimo, da B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Milano, 2022, p. 2. Il dato era già stato messo in luce, ad es., da G. DI PAOLO, "*Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2008, p. 13-16.

[70] Si pensi alla possibilità di ricorrere al deposito telematico via *pec* degli atti di denuncia e querela.

[71] Per un approfondimento su questo specifico punto, v., per tutti, B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica*, cit., *passim*.

– avvenga non più, o non soltanto, attraverso la «*percepti̇òn intuitiva humana*»[72] – ossia nelle strade delle città –, bensì negli uffici delle Procure e, più precisamente, attraverso i *computer* e i *tablet* posizionati sulle scrivanie dei pubblici ministeri e della polizia giudiziaria. I *device* digitali, sfruttando le potenzialità delle "connessioni di rete", sono in grado di compiere ogni attività utile al reperimento delle fonti di prova[73]. La metamorfosi della fase investigativa costituisce, dunque, un dato ormai acquisito: solo chi sia pervaso da un «tecnofobico […] *horror novi*»[74] potrebbe non rendersi conto del mutamento radicale che ha interessato – e sta tutt'ora interessando – il processo penale nell'era digitale.

Le statistiche avallano quanto qui sostenuto. Dalla lettura dell'ultimo *report* redatto dal *National Police Chiefs Council*[75], ad esempio, si può apprendere che circa il 90% dei procedimenti penali aventi ad oggetto reati commessi sul territorio inglese vengono accertati ricorrendo a mezzi di ricerca della prova aventi una componente intrinsecamente digitale. Nello stesso senso si è espressa pure la Commissione europea nella Raccomandazione di Decisione del Consiglio che ha autorizzato l'avvio di negoziati in vista di un accordo tra l'Unione europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche, ove si afferma che queste ultime sono oggigiorno necessarie per lo svolgimento dell'85% delle indagini penali[76].

Se questo è lo stato dell'arte, il punto problematico, come osservato a più riprese dai commentatori, è che quanto descritto è stato «seguito, finora, da un'insufficiente presa d'atto in sede legislativa, giurisprudenziale e dottrinale»[77]. In realtà, il Parlamento italiano è più volte intervenuto – ancorché in modo frammentato – nell'ottica di disciplinare il rapporto tra i nuovi strumenti informatici e il rito penale, con l'obiettivo di predisporre un vero e proprio "modello processuale differenziato" per l'accertamento dei reati commessi in Rete[78].

Per un verso, il legislatore si è mosso nell'intento di garantire un'efficace attività investigativa: sul presupposto che la previgente disciplina non fosse idonea a contrastare il

---

[72] Così, nel descrivere questo fenomeno, S. BARONA VILAR, *Algoritmizaciòn del derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Valencia, 2021, p. 598.

[73] Sul punto, v. quanto osservato da G. CECANESE, *Le pre-investigazioni informatiche e i controlli sui* social, in A. Scalfati (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Torino, 2020, p. 270: «oggi […] l'inquirente non esce più sul territorio – o per lo meno esce sempre meno – poiché l'acquisizione delle informazioni tende a realizzarle tutte all'interno dell'ufficio attraverso l'utilizzo del *computer* e di sistemi informatici capaci di controllare la vita, gli spostamenti e le abitudini di ogni individuo».

[74] G. DI CHIARA, *Il canto delle sirene*, cit., p. 23. Già anni or sono, illustre dottrina, disquisendo in merito al rapporto tra processo e informatica, ebbe ad affermare che, in questo settore, «resistenze e diffidenze non trovano giustificazione alcuna, né nella forza di inerzia, né altrove. Esse urtano inesorabilmente contro la realtà e contro la logica» (G. CONSO, *Macchine elettroniche e nuove prospettive giuridiche*, in *Riv. it dir. proc. pen.*, 1971, p. 661).

[75] NATIONAL POLICE CHIEFS COUNCIL, *Digital Forensic Science Strategy*, luglio 2020, p. 13.

[76] COMMISSIONE EUROPEA, *Recommendation for a Council Decision. Authorising the Opening of Negotiations in View of an Agreement between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters*, 5 febbraio 2019, p. 1.

[77] R. ORLANDI, *Questioni in tema di processo penale e informatica*, in *Riv. dir. proc*., 2009, p. 129. Rileva, altresì, come «l'evoluzione legislativa non [abbia] seguito di pari passo quella tecnologica», M. PITTIRUTI, Digital evidence *e procedimento penale*, Torino, 2017, p. 5.

[78] L. LUPÁRIA, Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, diretto da G. Spangher, vol. VII, *Modelli differenziati di accertamento*, Tomo I, a cura di G. Garuti, Torino, 2011, p. 369, il quale si riferisce a «un ordito infra-codicistico finalizzato a regolamentare, con caratteri di marcata autonomia, l'accertamento dei reati informatici».

nuovo fenomeno criminale in atto, sono andate emergendo tecniche investigative innovative, capaci di cogliere i riflessi processuali dell'immaterialità e della volatilità del dato digitale, carattere intrinseco della *digital evidence*[79]. Lungi dal ritenere le indagini informatiche circoscritte al settore della criminalità "a mezzo *Internet*", infatti, ci si è presto resi conto delle innumerevoli potenzialità che la Rete avrebbe potuto offrire agli organi investigativi per il contrasto di qualunque tipologia di illecito[80].

Per altro verso, è emersa contestualmente l'urgenza di tutelare il diritto dell'imputato a confrontarsi con il dato informatico[81], manifestazione moderna del diritto garantito all'art. 24, comma 2, Cost. Si tratta, più in generale, di una prerogativa che pare ricollegarsi all'adozione di un approccio volto a individuare un "giusto processo digitale"; un complesso di regole che, pur tenendo fermi i principi cardine del modello accusatorio, sia capace di adeguare le prerogative dell'imputato alle nuove sfide che il rito è chiamato ad affrontare nell'era informatica.

[79] Si pensi all'introduzione dell'art. 266-*bis* c.p.p. ad opera della l. 23 dicembre 1993, n. 547.

[80] Tra i primi ad aver messo in luce tale aspetto, v. L. LUPÁRIA, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in L. Lupária – G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 130 s.; R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, cit., p. 129; F. RUGGIERI, *Profili processuali nelle investigazioni informatiche*, in L. Picotti (a cura di), *Il diritto penale dell'informatica nell'epoca di* Internet, cit., p. 155, nt. 3.

[81] Cfr. P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc*., 2009, p. 406, che parla di una vera e propria «trasposizione moderna del diritto a confrontarsi con l'accusatore».

CAPITOLO II

I *SOCIAL NETWORK SITES*: RIFLESSI GIURIDICI DI UNA NUOVA CATEGORIA INFORMATICO-SOCIOLOGICA

SOMMARIO: 1. Inquadramento teorico dei *social network sites*: definizioni e delimitazioni concettuali. – 2. L'approccio della scienza giuridica al cd. "diritto dei *social network*": brevi cenni. – 3. Piattaforme digitali e diritto penale: verso una nuova *species* di illeciti *online*?

1. Inquadramento teorico dei *social network sites*: definizioni e delimitazioni concettuali

Nel contesto della moderna e frenetica comunità *hi-tech* è attualmente in corso un mutamento profondo, strutturale e radicale delle modalità attraverso le quali *Internet* consente ai propri utenti di interagire tra loro. Nel solco tracciato dalla tecnologia *web* 2.0[1], più in particolare, si è andato sviluppando un nuovo paradigma sociale e comunicativo basato su piattaforme digitali comunemente denominate *social network site*s[2].

Per cercare di stabilire i riflessi di questo nuovo fenomeno sul versante giuridico in generale, e sul sistema di giustizia penale in particolare, l'analisi deve necessariamente muovere da alcune precisazioni di carattere concettuale. Del resto, se è vero che «prima di applicare la legge, dobbiamo sviluppare un'immagine mentale dei fatti esistenti su cui essa possa essere applicata»[3], occorre avere ben chiaro quali siano le caratteristiche, il funzionamento e l'origine del "formante tecnologico" di cui si discute. Per tale ragione, prima di affrontare il tema centrale di questa ricerca, occorre fare chiarezza sull'esatto significato di talune espressioni che spesso vengono usate come sinonimi, ma che, in realtà, andrebbero tenute distinte.

Si proceda con ordine.

Con la locuzione *social network sites* si è soliti alludere a quella sub-categoria dei nuovi *media*[4] che, sfruttando le potenzialità del *web 2.0*, consentono a ciascun individuo di connettersi e comunicare con una cerchia indeterminata di soggetti (accomunati dai più

[1] Cfr. Parte I, Cap. I, par. 2.

[2] In un documento redatto dall'*European Network and Information Security Agency* in merito ai riflessi giuridici di queste nuove piattaforme digitali è stato osservato come esse rappresentino «*one of the most remarkable technological phenomena of the 21st century*» (EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA), *Security issues and Recommendations for on line social networks*, 2007, p. 6). Di «uno dei più recenti ed eclatanti effetti dell'impatto di *Internet* sulle relazioni interpersonali» ha parlato anche L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei* social network. *Aspetti penali*, in *Giur. mer*., 2012, p. 2522.

[3] O.S. KERR, *The Problem of Perspective in Internet Law*, in *Georgetown Law Journal*, 2003, p. 364 (trad. nostra).

[4] Il *medium* è uno strumento che consente all'essere umano di superare i vincoli e i limiti di una comunicazione *de visu*. In questa prospettiva, è possibili distinguere i cd. *Legacy media* (*media* tradizionali) dai cd. *New media*: nella prima categoria possono essere ricompresi la stampa, la radio e la televisione; nella seconda, invece, è possibile annoverare *Internet*, i *social network* e gli *smartphone* (T. FLEW, *New media: An introduction*, Oxford, 2008, p. 30).

disparati interessi: amicizia, lavoro, *hobbies*, etc.[5]), in modo tale che ogni utente sia messo nella condizione di creare e/o modificare la propria esperienza sociale. Si è al cospetto di quella che può essere definita come una forma di "comunicazione partecipativa immediata", in quanto ciascun cibernauta può offrire il proprio contributo nella diffusione di dati e informazioni, senza la necessità di intermediazioni operate da terzi. In tal modo, i *social network sites* offrono all'utente la possibilità di condividere idee e pensieri in maniera più rapida e molto meno dispendiosa di quanto avvenga *de visu*, superando tutte quelle barriere geografiche imposte da limiti fisici e, soprattutto, di avere un controllo totale (ma, al tempo stesso, apparente) sulla tipologia di dati che intende condividere, contribuendo così alla creazione di un «"Sé ideale" in formato *social*»[6].

La loro diffusione a livello globale[7] ha messo in discussione tanto le categorie tradizionali concepite dalle scienze sociali, quanto quelle create dalla scienza giuridica. D'altra parte, com'è stato efficacemente osservato, «*no existe en la historia de la humanidad un fenomeno social de tanto impacto que haya evolucionado en tan poco tiempo y con la magnitud que lo han hecho estas plataformas*»[8].

Effettivamente, questi *media*, sfruttando connessioni alla Rete sempre più veloci ed efficienti, hanno finito per rivoluzionare il *modus comunicandi* e, di riflesso, il comportamento sociale dell'uomo contemporaneo. Per rendersene conto è sufficiente volgere lo sguardo alle più recenti analisi statistiche relative all'utilizzo di *Facebook*, *YouTube*, *Instagram*, *WeChat* e dei numerosi altri *social website*. Nel giugno 2023, queste piattaforme hanno registrato un picco di 4,9 miliardi di utenti, ovverosia circa il 60,5% della

[5] Alla luce di ciò, in dottrina viene generalmente prospetta la distinzione tra *i*) reti sociali di comunicazione, quali, ad esempio, *Facebook*, *Tuenti* o *WhatsApp*, *ii*) reti sociali specializzanti, come *Genoom* o *Micueva* e *iii*) reti sociali professionali (si pensi, in via meramente esemplificativa, a *Linkedin*). In realtà, è stato osservato come non sia possibile addivenire a una classificazione esaustiva a fronte di un fenomeno, quello dei *social network sites*, in costante evoluzione (L. DAVARA FERNÁNDEZ DE MARCOS, *Implicaciones Socio-Jurídicas de las Redes Sociales*, Cizur Menor, 2015, p. 104).

[6] M. FASOLI, *Cacciatori (di informazioni) e prede (di trappole cognitive) nel* web 2.0*: una lettura cognitivo-evoluzionista dell'attrattività dei* social network, in *Sistemi intelligenti*, 2019, p. 400. Cfr. pure L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, p. 67.

[7] Una prima forma embrionale di *social network* può essere identificata nell'applicazione *SixDegrees.com*. Nata nel 1997 grazie all'intuizione dell'americano Andrew Weinreich, essa consentiva agli utenti di creare profili e connettersi con i propri amici, promuovendo così una primigenia forma di "incontri virtuali". È solo agli inizi del nuovo millennio, però, che, sulla scorta delle numerose opportunità, specialmente di natura economica, messe in evidenza da tale applicazione, alcuni visionari cominciarono a replicare tale modello. Nacquero così sistemi come *Ryze.com* (2001), *Friendster* (2002), *LinkedIn* (2002), *Myspace* (2003) e *Second Life* (2003). Il raggiungimento della fase di massima espansione dei *social network*, però, si ebbe solo con l'avvento di *Facebook*, il 4 febbraio 2004.

[8] A. PEREZ ESCODA – E. DANS, *La interacciòn social como mercancìa: redes sociales y plataformas*, in A. Perez Escoda – J. Rubio Romero (a cura di), *Redes Sociales ¿El quinto poder? Una aproximación por ámbitos al fenómeno que ha transformado la comunicación pública y privada*, Valencia, 2021, p. 30. Numerosi studi hanno cercato di mettere in luce le ragioni di quell'irresistibile attrattività propria dei *social network* che spinge miliardi di utenti ogni giorno a condividere informazioni sulla propria vita quotidiana. Tra i più accreditati, può essere ricordato quello di M. FISHER – R. BOLAND – K. LYYTINEN, *Social Networking as the Production and Consumption of a Self*, in *Journal of Information and Organization*, 2016, p. 131 ss., per i quali le ragioni legate al successo di questi nuovi *media* potrebbe essere riassunte in tre punti: a) il consumo di contenuti soddisfa i bisogni di informazione, intrattenimento e gestione dell'umore; b) l'interazione con gli altri utenti rafforza le connessioni sociali; c) la produzione di contenuti personali soddisfa i bisogni di autoespressione e autorealizzazione.

popolazione mondiale[9]: se *Facebook* fosse uno Stato sovrano, si è icasticamente osservato, «*it would be world's third largest country by population*»[10]. Un ulteriore dato significativo è quello relativo al rapporto tra internauti e fruitori dei *social network sites*: il 94% degli utenti di *Internet* è iscritto ad almeno una "rete sociale virtuale", cosicché circa il 90% delle attività condotte nel cyberspazio sono attualmente veicolate dalle piattaforme di *sharing*.

Le statistiche, dunque, dimostrano incontrovertibilmente come i canali gestiti dai *social network providers* costituiscono oggigiorno un imprescindibile strumento di "connessione sociale", finalizzato al mantenimento ovvero alla creazione di vere e proprie relazioni interpersonali[11]. I *social network sites*, in sostanza, sono ormai profondamente integrati nella vita quotidiana di ciascun individuo. Lo spasmodico bisogno comunicativo dell'era moderna[12] – che, ricorrendo a un'analogia con le espressioni "erbivoro" e "carnivoro", ha indotto a qualificare l'essere umano come «informivero»[13] – trova pieno appagamento in questi nuovi strumenti di comunicazione, creazione e condivisione di dati che implicano non solo «una "rivoluzione tecnologica", ma anche una riconfigurazione dei processi cognitivi, relazionali e sociali dei propri utenti»[14].

La disponibilità di uno spazio virtuale nel quale esprimere liberamente il proprio pensiero, dunque, pare aver spinto gli esseri umani verso la creazione di una comunità "virtuale" parallela e, talvolta, alternativa, a quella "reale". Anzi, com'è stato giustamente messo in luce, ciò che viene comunemente definita in termini di "realtà virtuale" è realtà a tutti gli effetti[15]; le esperienze vissute nel *web* non sono certo meno reali (o di seconda classe) rispetto a quelle vissute nell'universo materiale e corporeo che da sempre caratterizza l'agire umano. Ed è proprio per tale motivo che il combinato congiunto tra i *social network sites* e il cyberspazio ha trasformato quest'ultimo in un vero e proprio "luogo di vita sociale".

In realtà, occorre sottolineare come il fenomeno in esame risulti complesso, eterogeno e, soprattutto, di difficile inquadramento. Le numerose piattaforme digitali che offrono servizi

---

[9] Cfr. DATAREPORTAL, *Global social media statistics*, all'indirizzo *https://datareportal.com/social-media-users*.

[10] D. FLETCHER, *How Facebook is Redefining Privacy*, in *www.contenti.time.com*, 20 maggio 2010. E non stupisce, dunque, se una parte della dottrina americana ha definito il *social network* in questione come «*Facebookistan*», cioè la "nazione" degli utenti che utilizzano detta piattaforma (A. CHANDER, *Facebookistan*, in *North Carolina Law Review*, 2012, p. 1807 ss.).

[11] In questa direzione, risulta particolarmente felice e icastica l'espressione coniata dal sociologo ed esperto di nuove tecnologie Manuel Castells, il quale, per descrivere il cambiamento apportato dall'avvento dei nuovi *media* ha parlato di una «*network society*», ovverosia una società le cui fondamenta sono identificabili nella multilateralità delle relazioni intrattenute in Rete (M. CASTELLS, *Communication, Power and Counter-power in the Network Society*, in *International Journal of Communication*, 2007, p. 238 ss.).

[12] …che giustifica l'impiego di locuzioni quali "società della esibizione", dove tutto deve essere mostrato per apparire reale.

[13] G.A. MILLER, *Informavores*, in F. Machlup – U. Mansfield (a cura di), *The study of Information: Interdisciplinary Messages*, New York, 1986, p. 111 ss.

[14] G. RIVA, *I* social network, Bologna, 2016, p. 27, il quale soggiunge come la «riconfigurazione [sia] così profonda da mettere in discussione non solo le relazioni sociali ma anche la soggettività e la corporeità degli utenti dei *social network*».

[15] D.J. CHALMERS, *Più realtà. I mondi virtuali e i problemi della filosofia*, Milano, 2023, *passim*. Su questo aspetto, v. le penetranti considerazioni di S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, p. 395: «non siamo però di fronte a una persona virtuale, contrapposta a quella reale. È questo inedito intreccio che ci restituisce la persona concreta quale risulta dal suo attuale modo d'essere nel mondo, in una dimensione nella quale la rete gioca un ruolo di cui devono essere considerate le peculiarità».

di questo tipo, infatti, sono assai variegate, potendo spaziare dal settore professionale a quello ludico, fino a quello assistenziale[16]. Nonostante la loro diffusione, però, nella comunità scientifica non è ancora stata raggiunta una posizione unanime sulla qualificazione da attribuire a questi artefatti digitali.

Nell'approcciarsi allo studio della materia, può essere utile muovere dalla lettura di uno studio condotto da due ricercatrici americane che, per prime, hanno cercato di fornire una definizione di questo nuovo modo di comunicare. In un fortunato saggio del 2008, le studiose hanno descritto i *social network sites* come «*web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system*»[17]. Detto altrimenti, trattasi di uno spazio virtuale nel quale ogni partecipante crea o implementa la propria rete sociale mediante la comunicazione o la condivisione di informazioni con un numero potenzialmente indefinito di soggetti.

A ben vedere, la difficoltà nel rintracciare una nozione ampia e condivisa risulta già evidente laddove si conduca un'analisi di tipo lessicale. Tanto nel linguaggio scientifico, quanto in quello parlato, non è raro, in effetti, imbattersi in un utilizzo errato di espressioni differenti tra loro che, tuttavia, nell'ottica di chi le utilizza, aspirano a descrivere il medesimo fenomeno. Occorre sottolineare, infatti, come le locuzioni *social media*, *social network* e *social network site* (o *websites*) non siano affatto sinonimi.

Alcuni tra i più accreditati studiosi mondiali di *marketing* e comunicazione hanno definito i *social media* come «un gruppo di applicazioni basate su *Internet* che si fondano sulle basi ideologiche e tecnologiche del *web* 2.0, consentendo la creazione e lo scambio di contenuti generati dagli utenti»[18]. L'espressione *de qua*, richiamando il noto concetto di *medium*[19], pone chiaramente in evidenza la principale caratteristica di tali strumenti: si tratta di mezzi di "intermediazione sociale" che consentono la condivisione di contenuti testuali, immagini, video e audio con un pubblico globale.

La locuzione *social network*, invece, nasce e si sviluppa nell'ambito delle scienze sociali[20] e psicologiche con la finalità di descrivere e analizzare le multiformi relazioni tra individui,

[16] Per una enumerazione (e una breve descrizione) delle principali piattaforme di *social network sites* in uso nel mondo occidentale, v. L. DAVARA FERNÁNDEZ DE MARCOS, *Implicaciones Socio-Jurídicas de las Redes Sociales*, cit., p. 108-123.

[17] D.M. BOYD – N.B. ELLISON, *Social Network Sites: Definition, History, and Scholarship*, in *Journal of Computer-Mediated Communication*, 2007, 13, p. 211.

[18] A.M. KAPLAN – M. HEINLEIN, *Users of the World, Unite! The Challenges and Opportunities of Social Media*, in *Business Horizons*, 2010, p. 59 (trad. nostra).

[19] Cfr. *supra*.

[20] J. SCOTT, *Social Network Analysis*, in *Sociology*, 1988, p. 109 ss.

gruppi e organizzazioni sociali[21]. La cd. *social network analysis*[22], infatti, è quella branca delle scienze umanistiche volta alla comprensione del comportamento umano attraverso lo studio delle relazioni tra affini[23].

È all'interno di queste coordinate teoriche che nasce e si sviluppa l'espressione *social network websites*. L'interazione tra il concetto informatico di *social media* e quello sociologico di *social network*, grazie alle possibilità offerte dal *cyberspazio*, ha dato vita a una struttura (SNS) che consente di unificare «alcune caratteristiche delle reti sociali tradizionali – interazione, supporto e controllo sociale – con le caratteristiche del *web* – multimedialità, creazione e condivisone di contenuti»[24].

Alla luce di quanto osservato, le prospettive future sull'evoluzione dei *social network sites* sono presto tracciate: «*las redes sociales están aquí para quedarse*»[25]. Tali strumenti hanno cambiato il modo di comunicare e, dunque, di approcciarsi alla realtà. Essi non possono essere equiparate a semplici strumenti di svago o intrattenimento. Tutt'altro: si è al cospetto di artefatti tecnologici indispensabili e necessari per l'organizzazione politica, individuale e sociale della realtà circostante, indipendentemente dalla volontà degli individui di essere, o meno, connessi. I *social network sites*, in questa prospettiva, rappresentano un vero e proprio cambio di paradigma nel modo in cui le persone comunicano, condividono informazioni e intrattengono le proprie relazioni. Ma è proprio questo, a ben vedere, l'aspetto che rende così impervio il percorso volto a inquadrare, in termini giuridici, il fenomeno in parola: il diritto è chiamato a farsi carico delle proteiformi sembianze assunte dalla società, cercando di

---

[21] Invero, gli influssi della *SNA* hanno investito anche il settore criminologico. Numerosi studi, infatti, hanno attinto ai concetti fondamentali delle reti sociali per spiegare l'eziologia del comportamento criminale (cfr. M. WARR, *Companions in Crime: The Social Aspects of Criminal Conduct*, Cambridge, 2002, p. 3, il quale mette in luce come «*criminal conduct is predominantly social behavior. Most offenders are imbedded in a network of friends who also break the law, and the single strongest predictor of criminal behavior known to criminologists is the number of delinquent friends an individual has*»).

[22] La prospettiva della *Social Network Analysis* (SNA), a differenza degli approcci individualisti (*non-network explanation*) che cercano di comprendere i fenomeni sociali a partire dagli attributi individuali degli attori, non focalizza l'attenzione sul singolo individuo, bensì sull'ambiente sociale nel quale un individuo è inserito.

[23] La "rete interindividuale", dunque, può essere semplicemente definita come un insieme di persone accomunate da un particolare legame come, ad esempio, l'appartenenza al medesimo gruppo sportivo.

[24] G. RIVA, *I* social network, cit., p. 13 e, in part., p. 14, ove si mette in luce come «la principale novità dei *social network* è stata quella di permettere l'unione dell'esperienza sociale della nostra vita quotidiana con il cyberspazio, creando un nuovo spazio sociale ibrido che possiamo definire "interrealtà"». Ed è proprio questa interazione che ha indotto la Corte Suprema americana a coniare l'espressione «*modern Internet*», con ciò riferendosi a una nuova Rete caratterizzata in prevalenza dai *social websites* e vissuta attraverso gli stessi (*Packingham c. North Carolina*, 882 U.S. 2017). Lo strettissimo legame che oggigiorno intercorre tra questi due distinti fenomeni (*social media* e *social network*) è così evidente che anche uno tra i più autorevoli dizionari inglesi, l'*Oxford Dictionary*, sembra cadere in errore allorquando definisce i *social media* come «*websites and software programs used for social networking*», finendo così per sovrapporre la componente tecnologica a quella sociologica. Pure l'Enciclopedia Treccani, riferendosi al concetto di *social network*, si esprime erroneamente in termini di «servizio informatico *on line* che permette la realizzazione di reti sociali virtuali».

[25] F.S. PARRAT, *Redes sociales: Fenómeno Pasajero o Reflejo del Nuevo Internauta*, in *Cuadernos de comunicación e innovación*, 2008, p. 120. Nello stesso senso, v. J.P. SEMITSU, *From facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Government Surveillance*, in *Pace Law Review*, 2011, p. 380, per il quale «*like cars, social networking sites like facebook are not disappearing anytime soon*»; P.W. GRIMM – L.Y. BERGSTROM – M.M. O'TOOLE-LOUREIRO, *Authentication of Social Media Evidence*, in *American Journal of Trial Advocacy*, 2013, p. 437: «*social media is ubiquitous, and it is here to stay*».

risolvere i conflitti posti da un nuovo archetipo, le cui fondamenta non possono essere più rintracciate nei "vecchi" rapporti sociali *offline*.

2. L'approccio della scienza giuridica al cd. "diritto dei *social network*": brevi cenni

I concetti di "evoluzione tecnologica" e "mutamento sociale", come si è detto[26], si legano inscindibilmente a quello di "innovazione giuridica", intesa come la capacità del progresso scientifico e sociale di conformare il dettato normativo a esigenze prima inesistenti[27]. In effetti, deve riconoscersi che il diritto è, prima di tutto, un fenomeno sociale e, come tale, subisce i riflessi dell'evoluzione socioeconomica e, talvolta, ne influenza gli sviluppi. Per tali ragioni, dunque, non stupisce che, dal punto di vista giuridico, i *social network* siano classificabili alla stregua di una particolare tipologia di «servizi della società dell'informazione», così definiti all'art. 1, par. 2, della Direttiva 1998/34/CE[28], vale a dire come qualsiasi prestazione eseguita a distanza, normalmente dietro retribuzione, per via elettronica e fornita mediante trasmissione di dati su richiesta di un destinatario di servizi.

Ciò premesso, è interessante notare come oggigiorno ci si imbatta con una frequenza sempre maggiore in scritti e saggi dedicati proprio allo studio delle conseguenze *stricto sensu* giuridiche legate all'utilizzo delle *social webpages*[29]. Se è vero che non esiste un ramo del diritto che non sia stato profondamente coinvolto dalla rivoluzione digitale, le piattaforme *social* hanno senz'altro inciso sull'universo giuridico più di quanto sia possibile immaginare[30].

Tra i primi autori che si sono interrogati sulle interazioni tra i *social network* e il l'universo giuridico debbono essere ricordati, innanzitutto, gli studiosi di diritto costituzionale. Del resto, se l'avvento delle "connessioni di Rete" ha imposto un *upgrade* nell'interpretazione di numerose disposizioni della Carta Fondamentale[31], non v'è dubbio che la diffusione delle "reti virtuali" abbia posto il giurista contemporaneo dinnanzi a nuove sfide: «*ubi social, ibi ius*»[32]. Le peculiarità di tali strumenti, infatti, inducono a prospettare soluzioni differenti e

---

[26] Cfr. Parte I, Cap. I, par. 1.

[27] R. ROMANO, *Innovazione giuridica e diritto tecnologico. L'impatto del giurista nei modelli di progresso sociale e scientifico*, in *Life Safety and Security*, 2017, p. 104.

[28] Direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998 che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

[29] Cfr., ad es., K.L. OSSIAN, *Social Media and the Law*, New York, 2022; A. AGUSTINOY GUILAYN – J. MONCLÚS RUIZ, *Aspectos Legales de las Redes Sociales*, Madrid, 2021.

[30] A dimostrazione dell'assoluta novità di tale fenomeno e della crescente importanza che esso è destinato ad assumere, è interessante osservare, in una prospettiva empirica, come una semplice ricerca per parola su una delle principali banche dati giuridiche americane, *LexisNexis Legal Database*, riveli – nell'anno 2010 – la presenza di soli 10 casi nei quali è stato utilizzato o citato il termine *Facebook*; casi che salgono a 1.324 nel 2013 e a un numero imprecisato, superiore a 100.000, nel settembre 2023.

[31] T.E. FROSINI, *Il diritto costituzionale di accesso ad* Internet, cit., p. 24 s.: «da un punto di vista del diritto costituzionale, le tecnologie determinano nuove forme di diritti di libertà che, laddove non codificate, possono essere incardinate e quindi riconosciute nell'alveo delle tradizionali libertà costituzionali. Quindi, si possono interpretare le vigenti norme costituzionali ricavandone da esse le nuove figure giuridiche dei nuovi diritti di libertà».

[32] L'icastica locuzione è ripresa da M.R. ALLEGRI, Ubi Social, Ibi Ius. *Fondamenti costituzionali dei* social network *e profili giuridici della responsabilità dei* provider, Milano, 2018.

innovative rispetto a quelle già proposte per far fronte al cd. diritto di *Internet*[33]. Vi è chi, ad esempio, si è recentemente interrogato in merito alla riconducibilità delle *social network communities* nell'ambito delle "formazioni sociali" tutelate all'art. 2 Cost.[34].

Il diritto costituzionale non è, però, l'unica branca della scienza giuridica a essersi confrontata con l'impatto dei *social network*. Sul versante civilistico sono già numerosi gli studi dedicati alle possibili interazioni con i nuovi *media*, specialmente con riguardo al tema della natura giuridica del contratto sottoscritto tra l'utente-fruitore e il gestore della piattaforma[35].

Anche gli studiosi di diritto del lavoro hanno dovuto affrontare le conseguenze giuridiche della diffusione massiva delle piattaforme di *sharing*, con specifico riguardo al loro utilizzo come strumenti di controllo "a distanza" dell'attività lavorativa[36]. Grazie alle informazioni condivise su *Facebook* o *Instagram*, infatti, il datore di lavoro può conoscere le abitudini di vita, i gusti e i rischi per la salute del proprio dipendente, imponendo così al giurista di individuare nuovi limiti e cautele al potere di sorveglianza sul luogo di lavoro.

Da ultimo, è interessante dare conto dei riflessi del fenomeno in esame sul versante del diritto amministrativo. Le nuove opportunità che i *social network* hanno offerto alle pubbliche amministrazioni in termini di agevolazione e implementazione dei servizi per i cittadini sono state spesso accompagnate da nuove sfide per il giurista, specialmente a fronte di un utilizzo non sempre razionale di simili strumenti. Esemplificativo, in questa direzione, è il dibattito relativo alla valenza di una comunicazione a mezzo *social* realizzata da un esponente pubblico nell'esercizio della propria funzione istituzionale[37].

---

[33] In questa specifica prospettiva, v. P. PASSAGLIA, Privacy *e nuove tecnologie, un rapporto difficile. Il caso emblematico dei* social media, *tra regole generali e ricerca di una specificità*, in *Consultaonline.it*, 28 settembre 2016, p. 332 ss.

[34] Cfr., per una rassegna delle diverse opinioni, M.R. ALLEGRI, Ubi Social, Ibi Ius, cit., p. 29-37. Si pensi, ancora, al dibattito relativo alla legittimità dell'esercizio di un vero e proprio "potere censorio" da parte dei *social network providers*, destinato a incidere su alcuni diritti fondamentali garantiti dalla Costituzione, *in primis* sulla libertà di informazione, di espressione e di manifestazione del pensiero. Il noto caso di cronaca al quale si allude è quello relativo alla chiusura temporanea delle pagine *Facebook* riferibili a due partiti politici italiani, CasaPound e Forza Nuova, a seguito della pubblicazione di contenuti che, ad avviso del gestore della piattaforma, si ponevano in contrasto con la *policy* e gli *Standards* della *Community* adottati dal colosso statunitense. Il nodo gordiano, in questi casi, è rappresentato dalla necessità di operare un complesso bilanciamento tra esigenze di tutela della libertà imprenditoriale delle società che gestiscono i *social* e la libertà di espressone riconosciuta ai partiti politici.

[35] A livello monografico, si segnala, ad es., C. PERLINGIERI, *Profili civilistici dei* social networks, Napoli, 2014.

[36] Cfr., per una panoramica delle numerose questioni, M. FORLIVESI, *Il controllo della vita del lavoratore attraverso i* social network, in P. Tullini (a cura di), Web *e lavoro. Profili evolutivi e di tutela*, Torino, 2017, p. 37 ss.

[37] Sul versante nazionale, il caso più noto, divenuto famoso alle cronache, è quello che ha portato a una pronuncia della sesta sezione del Consiglio di Stato (Cons. Stato, Sez. VI, 12 febbraio 2015, n. 769). Ai fini della nostra analisi, è interessante sottolineare come la *quaestio iuris* oggetto di controversia concernesse il valore giuridico da attribuire a un *tweet* postato nel profilo privato del Ministro dei beni e della attività culturali che, nel giugno del 2013, aveva richiesto al Comune di La Spezia di sospendere i lavori di riqualificazione di una delle piazze principali della città. Al di là delle conclusioni alle quali sono giunti i giudici amministrativi – ovverosia, identificare la comunicazione via *social network* dei rappresentati istituzionali, alla luce del principio di tassatività degli atti amministrativi, come un mero atto politico a valenza interna – la vicenda *de qua* dimostra come l'utilizzo dei *social network* imponga nuove riflessioni attorno a categorie dogmatiche tradizionali – come, nel caso di specie, quella degli atti amministrativi e del principio di tipicità a esso correlato

Il breve – e necessariamente rapsodico – *excursus* in merito alla rilevanza assunta dalle nuove piattaforme digitali in alcune branche del diritto consente di mettere in luce la trasversalità del fenomeno in parola. Raramente, infatti, si è stati al cospetto di un'innovazione capace di incidere contestualmente e in maniera così significativa tanto sul versante socio-tecnologico, quanto sul versante giuridico nel suo complesso. Parafrasando le parole con cui autorevole dottrina ha descritto le conseguenze della «grande trasformazione tecnologica» nella società del XXI secolo, è possibile affermare, senza timori di smentite, che «[i *social network* stanno cambiando] il quadro dei diritti civili e politici, ridisegnando il ruolo dei poteri pubblici, mutando i rapporti personali e sociali, e incidendo sull'antropologia stessa delle persone»[38].

3. Piattaforme digitali e diritto penale: verso una nuova *species* di illeciti *online*?

L'avvento dei *social network* ha obbligato anche lo studioso di diritto criminale a confrontarsi con le innovazioni apportate da questi nuovi artefatti tecnologici. Muovendo dalla constatazione empirica per cui le moderne piattaforme digitali costituiscono il terreno più comune per la realizzazione di attività illecite nella Rete[39], la dottrina, specialmente nordamericana, si è interrogata, a più riprese, sulla possibilità di enucleare una vera e propria categoria di delitti definibili come *social network crimes*[40].

In un primo momento – che coincide, generalmente, con la diffusione delle comunità *online* nel panorama socioeconomico – la rilevanza penale di tali strumenti era perlopiù circoscritta al piano delle concrete modalità esecutive della condotta criminosa. In tale prospettiva, il fenomeno era descritto ricorrendo a espressioni quali *cybercrimes related to social media* o *cybercrimes on social network*. La piattaforma digitale, detto altrimenti, era considerata un mero strumento agevolatore per la commissione di condotte illecite già penalmente sanzionate dall'ordinamento[41]. Di conseguenza, la dottrina tendeva a inquadrare tali fattispecie nell'ambito della tradizionale categoria dei "delitti cibernetici": l'utilizzo delle piattaforme, infatti, presupponeva, in ogni caso, il ricorso a connessioni telematiche collocate nel cyberspazio[42].

– che, lungi dall'essere cristallizzate una volta per tutte, risentono degli influssi derivanti dal nuovo *modus comunicandi* del XXI secolo.

[38] S. RODOTÀ, *Una Costituzione per* Internet, in *Politeia*, 2006, p. 177.

[39] Si vedano le statistiche consultabili all'indirizzo *https://aag-it.com/the-latest-cyber-crime-statistics/*. Tra i delitti commessi "attraverso" i *social network*, meritano di essere espressamente menzionati quelli appartenenti alla categoria dei crimini di odio e di discriminazione. Cfr., *amplius*, F. BUENO DE MATA, *Investigación y prueba de delitos de odio en Redes Sociales: Técnicas OSINT e inteligencia policial*, Valencia, 2023, p. 28, al quale si rinvia per la disamina di specifici dati statistici sul punto.

[40] Si veda, in tal senso, K. LUTHER – R.M. HAYES, *#Crime: Social Media, Crime and Criminal Justice*, New York, 2018. Le prime riflessioni organiche sul panorama nazionale sono state offerte da L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei* social network, cit., p. 2522 ss.

[41] Questa visione è espressa in maniera chiara e puntuale nel *First Report Social media and Criminal Offences* commissionato dalla Camera dei Lord e pubblicato il 22 luglio 2014: «*here are two different ways to think about the harmful acts committed using social media: either they are new acts, or they are acts already prohibited by the criminal law but committed in the new forum of social media as opposed to elsewhere. We have been persuaded that the latter is usually the case*» (*https://publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/3702.htm*).

[42] In questi termini, L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei* social network, cit., p. 2525.

Con il passare del tempo, però, alcuni Autori, preso atto delle caratteristiche proprie dei nuovi mezzi di comunicazione elettronica, hanno cominciato a proporre differenti classificazioni, con lo scopo di evidenziare le peculiarità delle attività criminose poste in essere sui *social network*. Tra questi, vi è chi ha suggerito di distinguere – nell'ambito della macrocategoria dei *social media crimes* – tra le ipotesi nelle quali la piattaforma è utilizzata per trasmette informazioni a un pubblico indefinito o entrare in contatto con possibili vittime, da quelle in cui il ricorso a tale strumento è finalizzato alla raccolta di informazioni utili per la realizzazione di successive attività criminose[43].

All'interno della prima categoria, poi, occorrerebbe ulteriormente distinguere tra gli *online social network crimes* e i gli *offline social network crimes*.

Con la prima espressione, ci si riferisce a tutte quelle condotte criminose la cui commissione si realizza direttamente sui *social network*, quali, ad esempio, il cd. *socialstalking*, la diffamazione su *Facebook* o le minacce contenute in un "cinguettio" postato su *Twitter*. A tal proposito, tuttavia, sembra forse improprio parlare di veri e propri *social network crimes*, in quanto alcune tra le condotte in esame ben possono essere realizzate anche attraverso altri strumenti, come un semplice messaggio inviato da uno *smartphone*. Nel secondo sottogruppo rientrano, invece, quelle ipotesi in cui la condotta tipica del reato è materialmente realizzata *offline* e il *social network* rappresenta un mero veicolo utilizzato dal reo per interagire con la vittima o con terzi. È il caso dei numerosi crimini (lesioni personali, violenze sessuali e omicidi aggravati) commessi sfruttando canali telematici quali, ad esempio, *Craigslist*[44]. Anche in questo caso, però, il ricorso all'espressione *social network crime* non appare pienamente convincente. Si è al cospetto, più correttamente, di ipotesi in cui i nuovi mezzi di comunicazione costituiscono semplici elementi agevolatori della condotta criminosa, ovverosia meri «comportamenti preparatori, accessori o strumentali», come tali inidonei a far ritenere integrati gli elementi costitutivi del fatto di reato[45].

Per quanto concerne, ancora, la seconda categoria (*rectius*, le ipotesi nelle quali i criminali utilizzano i *social network* per raccogliere informazioni), occorre nuovamente distinguere

---

[43] T.A. HOFFMEISTER, *Social Media in the Courtroom. A New Era for Criminal Justice?*, Santa Barbara, 2014, p. 13 ss. Più semplicistica, ma non per questo meno efficace, la classificazione proposta da P. CIPOLLA, Social Network, *furto di identità e reati contro il patrimonio*, in *Giur. mer*., 2012, p. 2683, ove si distingue tra «reati favoriti dai *social network*, in cui *Facebook*, *Twitter* ecc. fungono da mere occasioni di contatto personale […] laddove il comportamento penalmente rilevante (il fatto tipico) è successivo al contatto virtuale ed è posto in essere nella sfera materiale" e "reati commessi nell'ambito e mediante i *social network*, laddove il fatto tipico è realizzato, in tutto o in parte, nel *cyberspazio*».

[44] È quanto avvenuto nell'estate del 2011 in Ohio, quando due criminali, dopo aver pubblicato un annuncio di lavoro su detto *social network*, hanno attirato le vittime designate in luogo lontano da occhi indiscreti, per poi perpetrare su di esse violenze e abusi (*https://www.nytimes.com/2011/12/02/us/three-lured-to-death-in-ohio-by-craigslist-job-ad.html*). Si pensi, ancora, ai cd. *flash mob crimes*, ovverosia casi nei quali gli utenti di un *social network* (ad esempio, *Telegram*), dopo essersi accordati sfruttando canali di comunicazione criptati, si riuniscono per vandalizzare le aree urbane delle città.

[45] Riprendendo le considerazioni di L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in Id. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 56 s., utilizzate dall'A. per escludere dalla categoria dei *cybercrime* alcune particolari ipotesi di reato quali, ad esempio, l'associazione terroristica che operi mantenendo contatti e rapporti fra gli associati esclusivamente attraverso la Rete.

tra i casi in cui i dati così ricavati siano utilizzati per commettere «*modern crimes associate with the Internet*», da quelli in cui gli stessi vengano sfruttati per realizzare condotte criminose nel mondo reale («*traditional crime*»[46]). Si consideri, con riguardo al primo sottogruppo, il furto d'identità digitale o il delitto di sostituzione di persona posti in essere grazie a un'attività illecita di raccolta di informazioni personali. Con riferimento, invece, ai "crimini tradizionali", il pensiero corre a tutte quelle ipotesi di furto in abitazione nelle quali l'agente utilizza i *social network* – ad esempio, *Instagram* – per seguire virtualmente gli spostamenti del "bersaglio", potendo così entrare indisturbato nell'abitazione della vittima in sua assenza[47].

Ad uno sguardo più attento, però, le nuove funzioni di interazione messe a disposizione dagli informatici e dagli studiosi di *social marketing* che prestano la loro opera presso le grandi *Companies* della Silicon Valley consentono di individuare nuove attività illecite caratterizzate dalla presenza di una condotta esclusivamente virtuale (*online*). Nell'ambito dei *social network*, infatti, è possibile distinguere due tipologie di comportamenti comunicativo-relazionali[48]. Il riferimento corre, da un lato, ai cd. *pure speeches*, espressione con la quale si allude ai pensieri comunicati o verbalizzati mediante la scrittura come, ad esempio, il contenuto di uno *status* di *Facebook* o di un *tweet*, o, ancora, il commento a una foto pubblicata su *Instagram*; dall'altro, alle cd. *symbolic expressions*, cioè, tutte quelle forme comunicative che prescindono dal ricorso al sistema alfanumerico tradizionale.

Ancorché entrambe le categorie menzionate debbano essere inquadrate nell'ambito della manifestazione del pensiero tutelata all'art. 21 Cost.[49], i problemi più evidenti sorgono con riguardo alla seconda. Si allude al tema della rilevanza penale assunta dalle differenti tipologie di "interazioni sociali indirette" con le quali l'utente del *web* può manifestare il proprio pensiero: *like*, *emoticon*, *smiley*, *re-post* o *re-tweet*, solo per fare alcuni esempi. La difficoltà del loro inquadramento in termini giuridici deriva dal fatto che in tali circostanze «"la condotta" si smaterializza, rispetto ai connotati empirici di un movimento fisico o muscolare, o comunque di un "atto" esteriore dell'uomo in carne ed ossa»[50]. L'utilizzo di "pollici digitali", di "cuori cibernetici" e di "faccine telematiche" chiama lo studioso a confrontarsi, ancora una volta, con un nuovo modo di comunicare, al fine di decifrarne il contenuto e individuare la regolamentazione giuridica più appropriata.

---

[46] Per le due ultime citazioni, v. T.A. HOFFMEISTER, *Social Media in the Courtroom*, cit., p. 34.

[47] In proposito, si è icasticamente osservato come «*historically, criminal defendants looking to burgle a residence had to stake out the place or look for telltale signs that occupants were away, such as stacked up newspapers or mail. Today, burglasrs look to social media*» (T.A. HOFFMEISTER, *Social Media in the Courtroom*, cit., p. 36).

[48] D.S. HARAWA, *Social Media Thoughtcrimes*, in *Pace Law Review*, 2014, p. 366 ss. e, spec., p. 378.

[49] Si rivelano particolarmente interessanti, in questo senso, gli spunti provenienti dal dibattito sorto oltreoceano. Ancorché nella prima pronuncia in materia (*Bland v. Roberts*, 857 F. Supp. 2d 599, 604, 2012) la Corte avesse affermato che l'utilizzo, nell'ambito dei *social network*, di segni grafici non riconducibili alla scrittura non godesse della tutela apprestata dal primo emendamento, oggigiorno i commentatori sono perlopiù concordi nell'estenderne l'ambito applicativo anche con riguardo a tale forma di manifestazione del pensiero. Cfr. M.D. MCPARTLAND, *An Analysis of Facebook "Likes" and Other Nonverbal Internet Communication Under the Federal Rules of Evidence*, in *Iowa Law Review*, 2013, p. 445 ss.

[50] L. PICOTTI, *La nozione di «criminalità informatica»*, cit., p. 842.

Ma è proprio questo il nucleo del problema: l'interpretazione di detti segni linguistici, la loro decodificazione[51] o, meglio, l'individuazione del valore a essi attribuibile.

Si tratta di una questione che, perlomeno allo stato attuale, è stata trattato in maniera superficiale dalla giurisprudenza italiana, sottovalutando talune questioni che, invece, meriterebbero maggiore attenzione. L'apposizione di un *like* a un *post* pubblicato su *Facebook*, ad esempio, è stata irragionevolmente ritenuta espressione di una volontà divulgativa atta a giustificare l'integrazione delle condotte apologetiche e propagandistiche rispettivamente punite agli artt. 604-*bis* e 414 c.p.[52]. Per sostenere tali conclusioni, i giudici estensori, salvo rare eccezioni[53], si sono limitati a richiamare il funzionamento dell'algoritmo utilizzato dalle piattaforme che – al netto della sua indubbia opacità – garantirebbe una maggiore visibilità ai *post* con il numero più elevato di interazioni (*like*, *emoticons* etc.), senza interrogarsi, invece, sul significato formale e sostanziale assunto dalle stesse. Per tentare di decifrare la volontà comunicativa che si cela dietro a un'esternazione "per immagini", occorrerebbe, invece, fare riferimento alle linee guida periodicamente pubblicate dai gestori dei *social network*[54], nonché esaminare quegli studi scientifici e statistici in tema di *emoticons interpretations*[55], la cui lettura appare utile per comprendere problemi e criticità posti dalla cd. *criminal law of digital speech*.

Ciò che emerge, in estrema sintesi, è come, nonostante alcuni tentativi di "codificazione"[56], il significato di questi pittogrammi non possa dirsi univoco, occorrendo valutare caso per caso la portata del segno in relazione alle differenti fattispecie incriminatrici di volta in volta in rilievo[57]. In altri termini, non sembra che le "condotte virtuali" delle quali si è detto – ancorché non esprimano dei concetti a parole, bensì con delle piccole immagini – siano comunque idonee a rendere univocamente manifesto il pensiero di chi le utilizza[58], con tutto ciò che ne consegue sul versante punitivo-sanzionatorio.

---

[51] La questione si pone in termini meno complessi allorquando l'utilizzo di segni grafici è accompagnato dal ricorso a frasi o espressioni linguistiche verbalizzate mediante la scrittura. Cfr. Cass. pen., Sez. V, 14 dicembre 2022, n. 2251, avente ad oggetto uno dei primi casi italiani di *body shaming*, nel quale un soggetto era stato accusato di diffamazione aggravata per aver commentato un post su *Facebook* con espressioni lesive della dignità umana, ricorrendo anche all'utilizzo di «più *emoticon* simboleggianti risate».

[52] Cass. pen., Sez. V, 25 settembre 2017, n. 55418, nella quale si sottolinea la «funzione propalatrice svolta [dal "mi piace"]». *Contra*, Cass. pen., Sez. I, 6 giugno 2019, n. 41635.

[53] Cass. pen., Sez. I, 6 giugno 2019, n. 41635, cit.

[54] Nella "Sezione informativa" di *Facebook* può leggersi quanto segue: «cliccare Mi piace sotto a un *post* […] è un modo per far sapere alle persone che quell'elemento ti piace senza lasciare un commento».

[55] Cfr., per tutti, V. EVANS, *The Emoji Code. How Smiley Faces, Love Hearts and Thumbs Up Are Changing the Way We Communicate*, Londra, 2017.

[56] Come, ad esempio, la cd. *Emojipedia* (*https://emojipedia.org/*).

[57] Si consideri l'ipotesi della cd. diffamazione a mezzo *social network* realizzata mediante l'apposizione di un *like* su un *post* pubblicato da terzi.

[58] Valgano due esemplificazioni. L'*emoticon* denominata *folded hands*, che rappresenta due mani unite palmo a palmo, viene utilizzata con quattro differenti significati: scusarsi, ringraziare, pregare o dare il cinque. L'apposizione di un *like* a un *post* di cordoglio, ancorché generalmente espressione di apprezzamento, potrebbe esprime, all'evidenza, una qualche forma di partecipanza emotiva all'accaduto, senza alcuna connotazione denigratoria od offensiva (A. RODRÍGUEZ ÁLVAREZ, *¿Sobran las palabras? Los emojis como prueba en el proceso judicial*, in *Revista de la Facultad de Derecho de México*, 2019, p. 694).

CAPITOLO III

L'INCIDENZA DELLE PIATTAFORME DI *SHARING* NELLA GIUSTIZIA PENALE DEL XXI SECOLO

SOMMARIO: 1. L'impatto delle "reti sociali online" nel sistema di giustizia penale contemporaneo: tre possibili chiavi di lettura. – 2. *Social network* e principio di imparzialità. – 2.1 L'impiego delle moderne piattaforme di *sharing* da parte dei giudici. – 2.1.1 La comunicazione istituzionale. – 2.1.2 "*To post or not to post*": la comunicazione personale. – 2.1.3 Astensione, ricusazione e "*virtual friendship*": … in attesa di Strasburgo – 2.2 Campagne mediatiche sui *social network* e rimessione del processo: una diade problematica. – 3. Piattaforme digitali e libertà personale: dal "diritto di accesso" a *Internet* al "diritto all'utilizzo" dei *social network* – 3.1 Misure cautelari e *social webpages*: il divieto di avvicinamento ai luoghi frequentati dalla persona offesa (art. 282-*ter* c.p.p.). – 3.2 *Social network* e arresti domiciliari tra "funzione conoscitiva" e "attività comunicative". – 4. La metamorfosi del "sapere" processuale: le informazioni presenti nelle *web communities* quale "petrolio digitale" per le autorità investigative. – 4.1 *Drafting* normativo: tecniche di legislazione applicate alle nuove indagini informatiche (anche nei *social network*).

1. L'impatto delle "reti sociali *online*" nel sistema di giustizia penale contemporaneo: tre possibili chiavi di lettura

I momenti di possibile rilevanza assunta dai *social network* nel contesto della giustizia penale *lato sensu* intesa[1] sono tanto variegati da rendere impossibile (e, probabilmente, superflua) una compiuta e dettagliata analisi degli stessi. Al di là dei casi di maggior clamore mediatico[2] e di un impiego delle piattaforme digitali da parte delle forze dell'ordine come strumento di comunicazione e interazione con la collettività[3], è senz'altro una celere rassegna della giurisprudenza italiana più recente a offrire la casistica più interessante. Si pensi, a mero titolo esemplificativo, all'ipotesi in cui la valutazione di pericolosità dell'indagato ai fini dell'applicazione di una misura cautelare possa essere desunta dai "cinguettii virtuali" pubblicati su *Twitter*[4]; al caso di un riconoscimento fotografico operato mediante un'immagine tratta da *Facebook*[5]; o, ancora, al rilievo assunto da *Instagram* ai fini della corretta individuazione del *dies a quo* per la decorrenza del termine di proposizione della querela[6].

[1] Con tale espressione, si allude, in questa sede, alle diverse fasi che compongono l'*iter* conoscitivo del sistema penale: *intelligence*, prevenzione e accertamento procedimentale.

[2] Ci si riferisce ai noti – e sempre più frequenti – casi di cronaca nei quali un utente, per le ragioni più disparate, pubblica sulla propria pagina *web* immagini, video o commenti che integrano, di per sé, una fattispecie di reato.

[3] Al fine di garantire una presenza e una "voce" delle autorità pubbliche anche nel mondo virtuale, nel solco di quella *Community policing* che suggerisce una stretta collaborazione tra la polizia e la collettività per aumentare la sicurezza nella società, le forze dell'ordine di tutto il mondo hanno cominciato a impiegare i *social network* come strumenti di comunicazione istituzionale, anche al fine di accrescere la propria legittimazione sul territorio. In argomento, cfr., per una panoramica, M.L. BESHEARS, *Effectiveness of Police Social Media Use*, in *American Journal of Criminal Justice*, 2014, p. 489 ss.

[4] Cass. pen., Sez. IV, 9 gennaio 2018, n. 6539.

[5] Cass. pen., Sez. II, 12 settembre 2019, n. 42315.

[6] In un recente caso di cronaca, la Procura della Repubblica di Roma ha ritenuto tardiva la presentazione di una querela sul presupposto che la persona offesa fosse giunta a conoscenza del fatto criminoso mediante una

Al netto di tali specifiche situazioni, è possibile individuare almeno tre grandi filoni di indagine, emblematicamente rappresentativi dei vari e numerosi momenti di intersezione tra i *social network* e la giustizia penale.

In una prima prospettiva, le piattaforme digitali sembrano incidere sui principi fondamentali della tradizione giuridica processualpenalistica, costringendo lo studioso a interrogarsi sulla necessità di un *upgrade* interpretativo. Si rivela paradigmatico, in tal senso, il canone di imparzialità sancito all'art. 111, comma 2, Cost.: le nuove connessioni digitali – occorre domandarsi – rischiano forse di rendere ineffettivo uno dei cardini della giurisdizione penale (*facultas jus diciendi*)?

Da un differente angolo visuale, si scorge come, nell'era tecnologica, le libertà fondamentali legate all'impiego dei *social network* tendono ad assumere una consistenza sempre più significativa anche nel rito penale, un luogo sacro che, da sempre, rappresenta il terreno di elezione per lo scontro delle ragioni dell'autorità con le ragioni delle libertà fondamentali. La dipendenza delle piattaforme digitali dalle moderne connessioni di Rete, da questo punto di vista, ha contribuito all'emersione, pure in campo processuale, di una libertà di nuovo conio: il diritto di accesso a *Internet*[7]. Che lo si voglia intendere come strettamente funzionale alla tutela di altre prerogative costituzionali ovvero come garanzia indipendente, i suoi riflessi sul versante procedimentale, come si avrà modo di osservare, appaiono di assoluto rilievo.

Infine, il terzo – e, a ben vedere, più complesso – momento di intersezione riguarda il rapporto tra il sistema di giustizia penale e i *big data* prodotti dall'utilizzo dei *social network*. Con la prima espressione, si è soliti alludere a tutti quei macro-dati generati in ogni istante da persone o cose (cd. *Internet of Things*), a fronte di un utilizzo sempre più massivo di strumentazioni tecnologiche nella vita quotidiana di ciascun individuo. Si tratta, in altre parole, di un processo di immagazzinamento di dati le cui capacità di acquisizione, gestione e analisi superano quelle dei *software* e degli *hardware* tradizionali[8]. Nell'era del *data deluge*, ogni individuo è messo in condizione di comunicare con chiunque e in qualunque

notifica su *Instagram*. Secondo l'accusa, infatti, «la pubblicazione comporta una notifica per tutti i *followers* […], pertanto la querela appare presentata oltre i termini previsti». La conclusione, però, non appare convincente, perlomeno sotto un duplice profilo: *in primis*, non corrisponde al vero che il funzionamento del *social network* in questione preveda una "notifica personalizzata" a tutti i *followers* laddove l'utente posti o pubblichi un messaggio sulla propria pagina; *in secundis*, appare censurabile l'idea di equiparare una notifica *social* alla ricezione di una raccomandata o di una PEC, attività, queste ultime, in grado di accertare l'effettiva ricezione di un'informazione proveniente da terzi (*https://www.cyberlaws.it/2019/giustizia-e-social-network/*). In proposito, peraltro, è interessante notare come talune pronunce della giurisprudenza di legittimità sembrano aver introdotto una "presunzione pretoria di conoscibilità" in capo agli amici e ai *followers* con riguardo ai *post* e alle dichiarazioni rese pubblicamente dagli utenti nei *social network*. La Suprema corte, difatti, afferma che ai fini della individuazione del *dies a quo* per la proposizione della querela occorre fare riferimento «ad una data contestuale o temporalmente prossima» a quella in cui la frase o l'immagine lesiva è stata immessa sulla piattaforma digitale (cfr. Cass. pen., Sez. V, 30 aprile 2021, n. 22787, da cui è tratta la citazione; Cass. pen., Sez. V, 29 maggio 2015, n. 38099).

[7] Per una prima messa a fuoco, sul versante processuale, v. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 116-120.

[8] Questa è la definizione offerta da MCKINSEY GLOBAL INSTITUTE, *Big data: The Next Frontier for Innovation, Competition, and Productivity*, 2021, p. 1 (trad. nostra). Rientrano in tale categoria, ad esempio, le informazioni di connessione e di interazione legate all'impiego dei *social network*, i dati biometrici e, più in generale, qualsiasi prodotto digitale di attività realizzate in Rete.

parte del globo. Questi canali informativi generano flussi ingenti di dati, gestiti direttamente dalle grandi piattaforme che governano il *web* 2.0: la persona diviene così fonte di infinite informazioni che viaggiano nel cyberspazio grazie alla forza virale dei *social network* come *Twitter*, *Facebook* e *Instagram*[9]. In proposito, si è parlato, non a torto, di «*datafication*» per indicare proprio la trasformazione di svariati aspetti della realtà quotidiana (comunicazioni, interazioni sociali, etc.) in contenuti *online* "qualificati", utilizzabili per mappare le abitudini di vita di un soggetto[10].

La circostanza che le reti *Internet* e le connessioni uomo-macchina generino, registrino e gestiscano quantità sempre maggiori di dati potrebbe apparire, però, del tutto priva di interesse per il giurista contemporaneo (e per il processualista in particolare), da sempre restio a interagire con altre branche della scienza, specialmente quelle scientifico-informatiche[11].

Una simile conclusione, tuttavia, sarebbe alquanto superficiale.

La dottrina più attenta, infatti, ha già messo in luce come l'irrompere sulla scena del procedimento penale dei *big data* rappresenti «il banco di prova della modernità giudiziaria», esigendo una reinterpretazione di tutti gli «snodi dell'impianto codicistico e procedimentale»[12].

Tra questi, la fase delle investigazioni *lato sensu* intesa è, senza dubbio, quella maggiormente interessata dal fenomeno in parola. Le autorità di *law enforcement* e la polizia giudiziaria, a ben vedere, non possono oggigiorno prescindere dall'utilizzo di questa "merce" preziosa[13], tanto che non sembra eccessivo affermare che le moderne operazioni istruttorie realizzate nel contesto della giustizia penale si sostanzino, essenzialmente, in attività di raccolta, analisi ed elaborazione di *bit* digitali. È pressoché inevitabile, da questo punto di vista, che le informazioni estratte dai nuovi spazi virtuali di condivisione e comunicazione vengano sfruttate nella fase di prevenzione e di contrasto alla criminalità[14], con riguardo sia agli illeciti tradizionali, sia ai *computer crimes*. A tal fine, i dati appresi dai *social network* possono essere utilizzati come prova di attività delittuose commesse nella stessa piattaforma – come nel caso di una diffamazione a mezzo *Facebook* – o realizzate nel "mondo analogico", ma per il cui accertamento risulta comunque indispensabile acquisire materiale digitale presente in Rete.

---

[9] Sulla capacità dei contenuti pubblicati nelle piattaforme digitali di divenire "virali" e sui riflessi *stricto sensu* giuridici, v. R. GARCIA – T.A. HOFFMEISTER, *Social Media Law in a Nutshell*, in *School of La Faculty Publication*, 2017, p. 1 ss. e, spec., p. 12 ss.

[10] V. MEYER-SCHOENBERGER – K. CUKIER, *Big Data. A Revolution That Will Transform Ho We Live*, Oxford, 2014, p. 1.

[11] In un saggio del 1971 sul rapporto tra giuristi e informatica, illustre dottrina lamentava già «l'assenza degli studiosi italiani dalle competizioni scientifiche che la cibernetica ha instaurato» (G. CONSO, *Macchine elettroniche e nuove prospettive giuridiche*, in *Riv. it dir. proc. pen.*, 1971, p. 661).

[12] E.M. MANCUSO, *L'ingresso dei* big data *nel procedimento penale*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*, Milano, 2019, p. 171, da cui sono tratte le ultime due citazioni.

[13] Cfr., nuovamente, E.M. MANCUSO, *L'ingresso dei* big data *nel procedimento penale*, cit., p. 171, per il quale «la rielaborazione dei dati, anche in forma coordinata, è ormai uno strumento imprescindibile per la lotta alla criminalità».

[14] Analogamente si esprime, proprio con riguardo ai dati ricavabili dai *social network*, F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Milano, 2020, p. 5.

2. *Social network* e principio di imparzialità

Il principio di imparzialità, «connotato intrinseco dell'attività del giudice»[15], costituisce un carattere fondamentale della giustizia penale, rappresentando una delle colonne portanti della funzione di *ius dicere*. Ancorché la sua origine venga sovente annoverata «tra quei principi non scritti […] che formano una sorta di piattaforma di diritto naturale»[16], il canone in parola trova oggi esplicito riconoscimento non solo in numerose fonti internazionali, ma anche nella Carta delle Leggi[17]. Garanzia soggettiva[18] avente natura multifunzionale, l'imparzialità, distinta dalla terzietà[19], è definita ordinariamente come "assenza di pregiudizi e di partiti presi". Si tratta di un «valore-fine tutelato dall'ordinamento»[20] che costituisce il presupposto logico-necessario per assicurare un corretto esercizio della funzione giurisdizionale, senza il quale «tutte le altre regole e garanzie processuali perderebbero di concreto significato»[21]. In assenza di un giudice imparziale, in altre parole, non può darsi giusto processo.

Collocandosi nel solco di questo inquadramento teorico, è interessante chiedersi, ai fini del presente studio, se e come l'utilizzo delle nuove piattaforme di comunicazione abbia inciso (o possa incidere) sull'imparzialità di chi è chiamato a decidere sulla responsabilità penale dell'imputato.

Il tema può essere approcciato adottando due distinte prospettive.

Dal punto di vista "interno", occorre esaminare il modo in cui il giudice (organo e persona fisica) impiega i nuovi *website*, al fine di saggiare se gli istituti tradizionali a tutela

---

[15] In tal modo si è espressa Corte cost., 25 marzo 1992, n. 124. Non è fuor d'opera sottolineare come tale requisito sia riferibile esclusivamente alla figura del giudice e non anche a quella del pubblico ministero. Non appare affatto convincente la giustificazione – ancora oggi in uso – già addotta dal Guardasigilli nel corso della discussione per l'approvazione del progetto preliminare del codice di rito del '30, laddove si sosteneva che il pubblico ministero, ancorché «parte del processo penale», è comunque «un organo dello Stato e quindi sempre soggetto ai princìpi di legalità ed imparzialità» (Relazione del Guardasigilli al progetto preliminare di un nuovo codice di procedura penale, in *Lavori preparatori del codice penale e del codice di procedura penale*, vol. VIII, Roma, 1929, p. 21). La tesi, com'è noto, era sostenuta da V. MANZINI, *Trattato di diritto processuale penale italiano*, vol. I, Torino, 1925, p. 142, per il quale «la funzione del pubblico ministero» è «in sé stessa personalmente disinteressata e imparziale». Questo «grossolano errore interpretativo», come si è efficacemente osservato, muove da un'errata esegesi del concetto di "imparzialità"; secondo il Foschini, infatti, al termine *de quo* potrebbero essere attribuiti due distinti significati: «a) l'uno relativo alla rettitudine e a un equilibrato esercizio della funzione; b) l'altro relativo ad una trascendenza rispetto agli opposti interessi, insiti nella regiudicanda»: solo il primo è idoneo a definire il concetto di imparzialità così come contenuto nell'art. 111, comma 2, Cost. (G. FOSCHINI, *Il pubblico ministero in un processo penale a struttura giurisdizionale*, in *Justitia*, 1966, p. 40).

[16] È la tesi prospettata da A. GIARDA, *Imparzialità del giudice e difficoltà operative derivanti dall'incompatibilità*, in AA. VV., *Il giusto processo*, Milano, 1998, p. 35.

[17] Art. 10 della Dichiarazione universale dei diritti dell'uomo e del cittadino; art. 6, comma 1, CEDU; art. 14 del Patto internazionale diritti civili e politici; art. 47 della Carta dei diritti fondamentali dell'Unione; e, da ultimo, art. 111, comma 2, Cost.

[18] M. CHIAVARIO, *Processo e garanzie della persona*, vol. II, Milano, 1984, p. 44, il quale sottolinea come, da un lato, il principio *de quo*, se osservato dall'angolo visuale delle Carte internazionali, rappresenti un vero e proprio diritto umano, una garanzia della persona sottoposta a processo; dall'altro, però, l'imparzialità può essere vista anche come «cristallizzazioni d'interessi primari della collettività».

[19] Come ricorda autorevole dottrina, l'imparzialità attiene alla concreta funzione esercitata dal giudice nel processo, mentre la terzietà deve riferirsi allo *status*, ossia il piano ordinamentale" e organizzativo dell'ufficio giudicante (P. FERRUA, *Il giusto processo*, Bologna, 2007, p. 51).

[20] F.R. DINACCI, *Giudice terzo e imparziale quale elemento "presupposto" del giusto processo tra Costituzione e fonti sovranazionali*, in *Arch. pen.* web, 18 ottobre 2017, p. 6.

[21] Corte cost., 29 settembre 1997, n. 306.

dell'imparzialità risultino adeguati a garantire efficacemente il canone cristallizzato all'art. 111, comma 2, Cost. Dal punto di vista "esterno", invece, è interessante porsi il problema di quali possano essere i risvolti *stricto sensu* processuali dell'utilizzo massivo dei *social network* da parte del *quivis de populo*, con specifico riguardo a un istituto, la rimessione *ex* artt. 45 ss. c.p.p., notoriamente volto a tutelare l'imparzialità dell'Ufficio giudicante.

Sul primo versante, peraltro, non possono essere sottaciute pure le strette implicazioni che intercorrono con la presunzione di innocenza, nella peculiare declinazione di regola di trattamento *ad extra*, ovverosia come divieto di rappresentare pubblicamente l'indagato-imputato come colpevole *ante iudicatum*[22].

Le esternazioni (personali e istituzionali) di pensiero realizzate dai giudici nei *social network*, da questo punto di vista, sembrano collocarsi a pieno titolo nell'ambito di applicazione dell'art. 4 della Direttiva 2016/343/UE, volto a regolamentare i "riferimenti in pubblico alla colpevolezza" dell'indagato-imputato[23]. La disposizione, infatti, si riferisce espressamente alle «autorità pubbliche», locuzione nella quale ben possono essere inclusi pure gli organi giudicanti. A sostegno di tale conclusione muove il contenuto del considerando n. 17 del provvedimento comunitario, secondo cui detto concetto dovrebbe essere inteso come comprensivo di tutte le «autorità coinvolte nel procedimento penale […] quali le autorità giudiziarie, di polizia e altre autorità preposte all'applicazione della legge».

Come noto, la normativa europea è stata recepita nell'ordinamento italiano solo di recente, a seguito dell'approvazione del d.lgs. 188/2021[24]. Per quanto qui rileva, l'art. 2, comma 1 del decreto, nel disciplinare le "condotte comunicative" che le «autorità pubbliche» debbono tenere allorquando si riferiscano «pubblicamente» alla persona sottoposta a indagini o imputata in un procedimento penale, fa divieto di indicare tali soggetti come colpevoli fino a quando la responsabilità penale non sia stata accertata con pronuncia irrevocabile. In merito alla nozione di «pubblica autorità», il Governo, come risulta evidente, ha riproposto letteralmente quanto previsto dall'art. 4 della Direttiva, ragion per cui può ritenersi che l'espressione *de qua* debba intendersi quale sinonimo di organismo che esercita funzioni pubbliche, potendovi ricomprendere pure l'organo giudicante che realizzi condotte lesive della presunzione di innocenza attraverso i *social network*. Al fine di rendere effettiva la garanzia apprestata dall'art. 2, comma 1 del decreto, il legislatore italiano ha previsto che, salve le eventuali sanzioni di carattere penale o disciplinare, il pregiudizio al canone cristallizzato all'art. 27, comma 2, Cost. attribuisce il diritto in capo al soggetto leso di ottenere il risarcimento del danno, nonché la rettifica della dichiarazione resa dall'autorità pubblica[25].

---

[22] In tema, cfr., per tutti, P.P. PAULESU, *La presunzione di non colpevolezza dell'imputato*, Torino, 2009, p. 159 ss.

[23] J. DELLA TORRE, *Il paradosso della direttiva sul rafforzamento della presunzione di innocenza e del diritto di presenziare al processo: un passo indietro rispetto alle garanzie convenzionali?*, in *Riv. it. dir. proc. pen.*, 2016, p. 1835 ss.

[24] D.lgs. 8 novembre 2021, n. 132.

[25] Per approfondimenti, sia consentito il rinvio, anche per ulteriori riferimenti bibliografici, ad A. MALACARNE, *La presunzione di non colpevolezza nell'ambito del d.lgs. 8 novembre 2021, n. 188: breve sguardo d'insieme*, in *Sist. pen.*, 17 gennaio 2022.

2.1 L'impiego delle moderne piattaforme di *sharing* da parte dei giudici

Se è vero che i *social network* rappresentano, nell'attuale società digitale, un fondamentale e imprescindibile strumento di manifestazione del pensiero, di comunicazione e di relazione intersoggettiva, non appare ragionevole negare *sic et simpliciter* all'autorità giurisdizionale la possibilità di utilizzare questi artefatti tecnologici. Il giudice, d'altro canto, al pari di ogni altro cittadino, è un essere umano, un soggetto che vive nel proprio tempo; egli, in altre parole, «non è un'entità astratta, avulsa dal contesto della società», bensì «intrattiene [con essa] una serie più o meno ampia di relazioni e di rapporti»[26]. Diversamente argomentando, ne sarebbe pregiudicato il corretto esercizio della funzione giurisdizionale che, come ben noto, postula una "vicinanza" culturale tra il titolare del potere di *ius dicere* e i suoi destinatari.

Il cuore della questione sulla quale ci si interroga, dunque, non riguarda tanto l'*an*, bensì il *quomodo*. Il quesito potrebbe essere così sintetizzato: la tutela del principio di imparzialità, in un mondo ormai digitalizzato, passa anche attraverso l'individuazione di limiti di carattere normativo e/o deontologico all'utilizzo dei *social network* da parte del giudice?

Per meglio inquadrare il tema, è necessario distinguere a seconda che il *website* venga utilizzato come *medium* per una più efficace comunicazione istituzionale (*i*), ovvero come strumento in capo al singolo magistrato (*ii*).

2.1.1 La comunicazione istituzionale

Nel primo caso (*i*), le espressioni manifestate nella sede digitale devono ritenersi imputabili all'Ufficio giudiziario nel suo complesso; di conseguenza, la regolamentazione giuridica di dette attività può essere agevolmente rintracciata nella Delibera del CSM contenente le «Linee-guida per l'organizzazione degli uffici giudiziari ai fini di una corretta comunicazione istituzionale»[27]. Il citato provvedimento raccomanda, sia con riguardo agli uffici inquirenti, sia a quelli giudicanti, la designazione di un responsabile per i rapporti con la stampa e i terzi, in persona del capo dell'ufficio o, su delega di questo, del magistrato che abbia maggiori attitudini ed esperienze comunicative.

In realtà, va osservato come detta disciplina pare non aver recepito *in toto* le direttive provenienti dai più importanti organismi a livello comunitario quali, ad esempio, l'*European Network of Councils for the Judiciary* (ENCJ), il cui dichiarato obiettivo, tra gli altri, è quello di promuovere un «*pro-active (educational) attitude of the judiciary*»[28], al fine di garantire il rispetto dell'indipendenza giudiziaria nel contesto eurounitario.

A tal proposito, il recente *report* titolato "*Public Confidence and the Image of Justice Individual and Institutional use of Social Media within the Judiciary*", nella piena consapevolezza delle peculiarità che contraddistinguono la comunicazione "via *social"* rispetto all'utilizzo della stampa o dei *media* tradizionali (radio e televisione, *in primis*), ha sollecitato gli Stati membri a introdurre una regolamentazione *ad hoc*. Per un verso, si sottolinea la necessità che gli *accounts* istituzionali riferibili all'Ufficio giudiziario – la cui

[26] G. SPANGHER, *La rimessione dei procedimenti*, Milano, 1984, p. 2.

[27] Per un commento alla quale, si rinvia a G. CANZIO, *Un'efficace strategia comunicativa degli uffici giudiziari vs. il processo mediatico*, in *Dir. pen. proc.*, 2018, p. 1537 ss.

[28] *https://www.encj.eu/node/480*.

adozione è vivamente raccomandata – siano gestiti «*by trained and authorised online spokespersons of the institution*». Per altro verso, viene rimarcato come la comunicazione debba essere sempre effettuata nell'ambito «*of the strategies and as advised by the experts in communication*», cioè da veri e propri *social network manager*[29].

L'esigenza, avvertita a livello sovranazionale, di una collaborazione virtuosa tra magistratura ed esperti di *social media communication* ha importanti riflessi anche sul principio di pubblicità del processo penale *lato sensu* inteso, ovverosia come diritto della collettività a essere informata e dovere dell'autorità giudicante e inquirente di informare. Se è vero che il provvedimento giudiziario resta, ancora oggi, l'atto principale con il quale il decisore manifesta all'esterno (cioè, nei confronti del popolo, il soggetto in nome e per conto del quale la giustizia è amministrata, art. 101, comma 1, Cost.) l'azione della magistratura, non può ignorarsi, in una società iperconnessa, la necessità di incrementare le prestazioni comunicative con l'impiego di nuovi strumenti. Nell'attuale epoca storica, però, non sembra più sufficiente la mera previsione dell'obbligatorietà di una comunicazione istituzionale; ciò che occorre è, soprattutto, sapere divulgare le informazioni nei modi e nei tempi più opportuni, onde renderle concretamente fruibili alla collettività. Si tratta di un aspetto colto dal già citato *report* europeo, ove si sottolinea esplicitamente la necessità per la magistratura di adattare le proprie capacità di comunicazione alla realtà del XXI secolo[30].

In questa prospettiva, potrebbe farsi riferimento al modello recentemente implementato nell'ordinamento spagnolo, nel quale la comunicazione istituzionale dell'Ufficio giudiziario è affidata alle *officinas de prensa*, cioè veri e propri dipartimenti stampa gestiti da esperti di *social media communication*. Una relazione diretta tra giornalisti e magistrati, peraltro, potrebbe forse contribuire a limitare quella pratica odiosa (e, perlopiù, impunita) consistente nel passaggio informale di notizie riservate sull'andamento delle indagini preliminari.

2.1.2 "*To post or not to post*": la comunicazione personale

Più complessa appare l'ipotesi sub *ii*), non fosse altro perché, come rilevato da un recente documento elaborato dai giudici di Cassazione, «l'attività compiuta dai singoli magistrati sui *social network* non è […] oggetto di regolamentazione positiva, neppure nella forma di regole non vincolanti aventi funzione di direttive o raccomandazioni»[31].

Si tratta non solo di una scelta censurabile, ma anche in controtendenza rispetto alle recenti linee evolutive sul panorama internazionale. In effetti, numerosi Paesi europei, sulla scorta delle indicazioni offerte a livello comunitario dai più autorevoli organismi in materia[32], hanno provveduto ad aggiornare le linee guida nazionali in tema di *judicial conduct* proprio

[29] EUROPEAN NETWORK COUNCILS JUDICIARY, *Public Confidence and the Image of Justice Individual and Institutional use of Social Media within the Judiciary*, 7 giugno 2019, par. 3.3.

[30] EUROPEAN NETWORK COUNCILS JUDICIARY, *Public Confidence*, cit., par. 3.3.

[31] Trattasi del documento redatto in risposta a un questionario proveniente dalla Corte Suprema della Repubblica Ceca sull'utilizzo delle piattaforme digitali da parte dei magistrati: *Risposte della Corte Suprema di cassazione al questionario proveniente dalla Corte Suprema della Repubblica Ceca sulle attività secondarie e l'uso dei social media da parte dei magistrati*, 30 settembre 2021, p. 8.

[32] EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE, *Guide on Communication with the Media and the Public for Courts and Prosecution Authorities*, 2018.

al fine di introdurre specifiche previsioni contenenti avvertenze e limiti per un impiego più accorto e saggio da parte dei giudici delle nuove piattaforme digitali[33].

A fronte di tale vuoto normativo e regolamentare, l'interprete sembra essere chiamato a individuare un punto di equilibro tra contrapposti interessi di rango costituzionale[34].

Per un verso, non può dubitarsi del fatto che la libertà di opinione e di manifestazione del pensiero – cui i *social network* contribuiscono oggigiorno in maniera significativa, se non, financo, preponderante – sono condizioni indispensabili per il pieno sviluppo di qualunque persona (e, pertanto, anche del giudice), ponendosi a fondamento di ogni società libera e democratica. Parimenti, la libertà di associazione (art. 21 Cost.) e la parità di trattamento di tutti i cittadini (art. 3 Cost.), come si è ricordato, non possono che trovare piena esplicazione anche nel contesto digitale.

Epperò, per altro verso, non può neppure negarsi che l'avvento dei *social media* abbia inciso sul canone cristallizzato all'art. 111, comma 2, Cost., nella specifica declinazione della cd. imparzialità apparente, ovverosia la rappresentazione pubblica della funzione giudiziaria. Cardine della giustizia moderna, il principio in esame viene in rilievo, sotto tale profilo, in quella che la Corte europea ha definito la cd. dimensione soggettiva o imparzialità personale[35]: ai sensi dell'art. 6, par, 1 CEDU, il giudice deve "essere" non solo imparziale, ma anche "apparire" come tale[36]. Per raggiungere tale obiettivo – insegnano i giudici europei – occorre sanzionare tutte quelle condotte soggettivamente riferibili al giudice dalle quali è possibile apprezzare il suo pensiero rispetto ai fatti oggetto della causa: ostilità manifeste o pesanti pregiudizi[37].

La necessità di stabilire un "momento di armonia" tra le opposte esigenze in gioco, del resto, emerge, sebbene in un contesto più generale, pure dalla lettura della nota sentenza n. 100/1981 resa dalla Corte costituzionale[38]. In quella sede, come si ricorderà, la Consulta ebbe modo di affermare che l'esercizio in capo al giudice del diritto di manifestare il proprio pensiero può essere limitato in ragione del contrapposto valore di rango costituzionale (si legga, l'imparzialità) solo qualora venga esercitato in maniera anomala, cioè abusiva.

---

[33] Si vedano, ad esempio, le nuove *guidelines* adottate nell'ordinamento inglese: *Guide to Judicial Conduct*, 2023, p. 20 s.

[34] Un'attività ermeneutica che, com'è noto, si differenzia dal cd. bilanciamento. Quest'ultimo, infatti, «non mira tanto all'equilibrio tra valori o interessi in conflitto», bensì all'individuazione di «una relazione di precedenza condizionata, concreta e relativa, in cui le condizioni in base alle quali un interesse precede un altro costituiscono il presupposto di fatto della regola che in concreto consente di giustificare l'ordine di priorità stabilito» (così, A. MORRONE, *Il custode della ragionevolezza*, Milano, 2001, p. 301 s.).

[35] Cfr. Corte edu, 6 maggio 2003, *Kleyn e altri c. Paesi Bassi*, par. 191; Corte edu, 6 novembre 2003, *Zennari c. Italia*. Al contrario, la cd. dimensione oggettiva richiama l'attenzione a quelle ipotesi in cui il giudice abbia anteriormente esercitato, in concreto, uno specifico potere tale da pregiudicare la vicenda processuale oggetto di giudizio: cfr., il *leading case*, Corte edu, 1° ottobre 1982, *Piersack c. Belgio*.

[36] L'esigenza di garantire un'apparente imparzialità fu affermata espressamente e per la prima volta, nel contesto nordamericano, da Lord Hewart nel caso *Re v. Sussex Justices Ex parte McCarthy* 1924, 1 KB 256, 259: «*justice should not only be done but should manifestly and undoubtedly be seen to be done*».

[37] Cfr. Corte edu, 28 febbraio 2003, *Lavents c. Lettonia*, par. 117; Corte edu, 26 ottobre 1984, *De Cubber c. Belgio*.

[38] Corte cost., 8 giugno 1981, n. 100.

Alla luce di tali coordinate, parte del problema nell'analizzare il tema in esame sembra riconducibile alla tendenza degli studiosi – e dei numerosi organismi di etica professionale – ad arroccarsi su visioni preconcette, come tali non condivisibili[39].

Da un lato, un approccio restrittivo vorrebbe negare *tout court* o, quantomeno, limitare fortemente, l'utilizzo dei *social network* da parte del singolo giudice-persona fisica. Tuttavia, come ricordato nella Dichiarazione di Doha recante le linee guida sull'utilizzo dei *social media* da parte della magistratura, i giudici «sia come cittadini che nell'esercizio delle loro funzioni giudiziarie, [sono] coinvolti nelle comunità che servono»[40]. Di conseguenza, negare a monte l'utilizzo di dette piattaforme risulterebbe non solo lesivo di diritti aventi rango costituzionale, ma, altresì, giuridicamente irragionevole: lo si ripete ancora una volta, un giudice che non vive nel contesto sociale che lo circonda è un giudice che, molto probabilmente, non rende Giustizia.

Dall'altro, una visione permissiva ritiene sufficiente affidare esclusivamente all'autoregolamentazione di settore l'individuazione di eventuali limiti all'impiego delle piattaforme di comunicazione.

Al netto di un'eventuale rilevanza deontologica e disciplinare derivante dall'utilizzo improprio delle piattaforme di *social network*[41], ciò che qui interessa approfondire sono le possibili conseguenze sul piano *stricto sensu* processuale. In altri termini, occorre chiedersi se le variegate attività *online* realizzabili dal giudice (persona fisica) possano avere una qualche rilevanza con riguardo agli istituti volti a tutelarne l'imparzialità.

2.1.3 Astensione, ricusazione e "*virtual friendship*": … in attesa di Strasburgo

Posti a tutela dell'imparzialità del giudice inteso come persona fisica, e derogando al principio enunciato all'art. 25 Cost., gli istituti dell'astensione e della ricusazione rappresentano strumenti processuali atti a «impedire che le passioni dell'uomo prendano il sopravvento sul retto sentimento del giudice»[42].

Fra le ipotesi previste agli artt. 36 ss. c.p.p., una in particolare sembra assumere astratta rilevanza qualora si tratti di stabilire se l'impiego personale da parte del giudice di un *social network* possa o meno avere ricadute sul versante processuale. Il riferimento va all'art. 36, comma 1, lett. c) c.p.p., ove viene presa in considerazione l'evenienza in cui il giudicante abbia manifestato il proprio parere sull'oggetto del procedimento «fuori dall'esercizio delle funzioni giudiziarie». Con tale espressione, com'è noto, la giurisprudenza si riferisce a tutte quelle esternazioni di impressioni, previsioni o giudizi manifestati all'esterno dell'aula di

[39] Per una panoramica, sul versante americano, cfr. S. VINCENT JONES, *Judges, Friends, and Facebook: The Ethics of Prohibition*, in *Georgetown Journal of Legal Ethics*, 2011, p. 286 ss.

[40] DICHIARAZIONE DI DOHA, *Linee guida non vincolanti sull'utilizzo dei* social media *da parte della magistratura*, 2019 (versione italiana).

[41] «Vorrei sottolineare come in questo ambito [quello della deontologia] una questione nuova, delle più delicate, è quella dell'uso dei *social media* da parte dei magistrati: si tratta di strumenti che, se non amministrati con prudenza e discrezione, possono vulnerare il riserbo che deve contraddistinguere l'azione dei magistrati e potrebbero offuscare la credibilità e il prestigio della funzione giudiziaria». Queste sono le parole pronunciate dal Presidente della Repubblica, Sergio Mattarella, all'inaugurazione dei Corsi di formazione della Scuola Superiore della Magistratura nell'anno 2019.

[42] E. CARBELLOTTO, voce *Ricusazione ed astensione del giudice e degli ufficiali del pubblico ministero* (dir. proc. civ. e dir. proc. pen.), in *Enc. giur.*, vol. XIV, Milano, 1906, p. 363.

giustizia in ordine al risultato di un determinato procedimento e attinenti, dunque, a un caso specifico[43]. Nessun dubbio, in proposito, che tali dichiarazioni possano essere rese anche *on the web*[44].

È, però, gettando lo sguardo oltre i confini nazionali che emerge come uno dei temi "caldi" sia rappresentato dalla possibilità di addurre la mera "amicizia" (ovvero, la qualifica di *follower*) su un *social network* come elemento a sostengo di un'istanza di ricusazione (e, prima ancora, di un obbligo di astensione). La rilevanza del tema – che, a prima vista, non parrebbe meritevole di seria considerazione – può cogliersi considerando come risulti attualmente pendente dinnanzi alla terza Sezione della Corte europea dei diritti dell'uomo un ricorso con il quale si chiede al giudice europeo di stabilire se l'amicizia su *Facebook* tra un giudice e una delle parti è compatibile con la garanzia di imparzialità prevista all'art. 6, par. 1 della Convenzione[45].

Si muova dal dettato normativo.

A mente dell'art. 36, comma 1, lett. h) c.p.p., il giudice ha il dovere di astenersi qualora sussistano «gravi ragioni di convenienza» che lo inducano a ritenere necessario, nel caso di specie, dismettere l'esercizio della funzione giurisdizionale. A tale riguardo, verrebbe da chiedersi se la mera qualifica di "amico" sul *social network* possa assurgere a grave motivo idoneo a giustificare un obbligo di astensione.

Nel nuovo continente, la questione *de qua* è stata risolta in termini essenzialmente negativi[46], tanto dalle Corti federali, quanto dalle Associazioni forensi[47]. L'idea a sostegno di tale conclusione è agevolmente intuibile: un "amico" è una persona legata a un'altra da sentimenti di affetto o stima; al contrario, il semplice *follower* rappresenta una persona "collegata virtualmente" a un'altra per via digitale.

Nondimeno, va dato conto di un atteggiamento draconiano manifestato dall'*Advisory Committee* dello Stato della Florida, per il quale la semplice "amicizia digitale" tra un avvocato e un giudice potrebbe «ragionevolmente trasmette a terzi l'impressione che questi "amici" ricoprano una speciale posizione in grado di influenzare l'esito del giudizio»[48]. Tale conclusione è stata fatta propria dalla Corte Federale nel caso *Domville c. Stati Uniti*, ove i giudici hanno accolto l'istanza di ricusazione promossa dall'imputato e rinviato la causa al tribunale di prime cure sul presupposto che l'amicizia su *Facebook* tra il giudice e il *prosecutor* «avrebbe creato in una persona ragionevolmente prudente un fondato timore di

[43] Cfr., per tutte, Cass. pen., Sez. II, 4 novembre 2005, n. 766.

[44] G. MANTOVANI, *Informazione, giustizia penale e diritti della persona*, Napoli, 2011, p. 324.

[45] Corte edu, *Chaves Fernandes Figueiredo v. Switzerland (communicated case)* - 55603/18.

[46] Per una panoramica generale, cfr. J.G. BROWNING, *Why Can't We Be Friends? Judges' Use of Social Media*, in *University of Miami Law Review*, 2014, p. 487 ss.

[47] Cfr. AMERICAN BAR ASSOCIATION, *Formal Opinion 462 (2013)*; NEW YORK ADVISORY COMMISSION ON JUDICIAL ETHICS, *Opinion 13-39 (2013)*; NEW YORK ADVISORY COMMISSION ON JUDICIAL ETHICS, *Opinion 08-176 (2009)*; THE SUPREME COURT OF OHIO-BOARD OF COMMISSIONERS ON GRIEVANCES AND DISCIPLINE, *Opinion 7/2010*; SOUTH CAROLINA, ADVISORY COMMITTEE ON STANDARDS OF JUDICIAL CONDUCT, *Opinion 17-2009 (2009)*.

[48] FLORIDA SUP. CT., *Judicial Ethics Advisory Committee*, Op. 2009-20 (trad. nostra).

non ricevere un processo equo»[49]. La medesima linea esegetica, peraltro, è stata avallata anche nel documento redatto dal *United Nations Office on Drugs and Crime*, nel quale si è affermato, testualmente, che «*judges should avoid accepting or sending friend requests from or to parties or their legal representatives*»[50], invitando, di conseguenza, i giudicanti a monitorare periodicamente i propri *accounts* dei *social media* e adottare le misure necessarie per eliminare o modificare contenuti o pubblicazioni che potrebbero ingenerare un dubbio sulla parzialità del loro operato[51].

In una differente prospettiva si collocano, invece, due recenti pronunciamenti resi in sede civile dalla Corte di cassazione d'oltralpe[52]. In quella sede, i giudici francesi hanno precisato che il termine "amico" o *follower* utilizzato per designare le persone che accettano di entrare in contatto sui *social network* non può essere interpretato come indice di un vero e proprio "rapporto di amicizia" nel senso tradizionale del termine, giacché la piattaforma rappresenta un semplice mezzo di comunicazione tra persone che condividono interessi comuni.

Con riguardo al panorama nazionale, è senz'altro alla giurisprudenza amministrativa che occorre volgere lo sguardo.

Collocandosi nel solco dell'impostazione dominante oltreoceano (ma, come si è visto, affatto unanime), i giudici hanno affermato a più riprese come i codici di procedura civile e penale dettino principi molto chiari per quanto riguarda il dovere di astensione e l'eventuale ricusazione, avendo come canone di riferimento le cd. "frequentazioni abituali" dei magistrati. Muovendo da tale assunto, si è sostenuta l'irrilevanza delle mere "amicizie" su *Facebook* «in quanto lo stesso funzionamento del *social network* consente di entrare in contatto con persone che nella vita quotidiana sono del tutto sconosciute»[53]. In proposito, d'altro canto, non v'è chi non veda come nell'odierno modo di comunicare qualunque occasione conviviale anche del tutto episodica, «può essere "catturata" con il telefono cellulare e repentinamente pubblicata sul *social network*. Non può, questo, essere considerato indice di una commensalità abituale»[54].

L'interpretazione pretoria, peraltro, è stata recepita anche in una recente Delibera concernente l'uso dei mezzi di comunicazione elettronica e dei *social media* da parte dei magistrati amministrativi[55].

---

[49] *Domville c. Stati Uniti*, No. 4D12-556, 2013 WL 163429 (trad. nostra), nella quale si precisa che «*judges do not have the unfettered social freedom of teenagers*» e «*a person who accepts the responsibility of being a judge must also accept limitations on personal freedom*».

[50] UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Non-Binding Guidelines on the Use of Social Media by Judges*, 2019, punto n. 30. Nello stesso senso si è espressa la Corte Suprema della Namibia, *Ethical judicial conduct in Namibia*, p. 52, ove è stato considerato vietato il comportamento del giudice che invia richieste di amicizia agli avvocati, o che accetta tali richieste.

[51] UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Non-Binding Guidelines on the Use of Social Media*, cit., punto n. 26. In senso contrario, v., invece, l'opinione espressa dall'AMERICAN BAR ASSOCIATION, *Formal Opinion 462 February 21, 2013 Judge's Use of Electronic Social Networking Media*, p. 3: «*nothing requires a judge to search all of the judge's ESM connections if a judge does not have specific knowledge of an ESM connection that rises to the level of an actual or perceived problematic relationship with any individual*».

[52] Corte di cassazione francese, Sez. II civile, 5 gennaio 2017, 16-12.394.

[53] TAR Lazio, 5 gennaio 2011, n. 40.

[54] TAR Sardegna, 3 maggio 2017, n. 281. Da ultimo, nello stesso senso, Cons. Stato, 14 aprile 2022, n. 2849.

[55] Cons. Stato, *Delibera sull'uso dei mezzi di comunicazione elettronica e dei social media da parte dei magistrati amministrativi*, 25 marzo 2021.

Dopo aver affermato che detti soggetti – adottando elevati parametri di continenza espressiva e utilizzando un linguaggio adeguato e prudente – «possono utilizzare i *social media*, nella propria vita privata, anche attraverso pseudonimi»[56], si afferma che «le amicizie sui profili *social* non costituiscono un elemento di per sé rilevante a manifestare la reale consuetudine di rapporto personale richiesta ai fini delle incompatibilità». A seguire, però, i redattori del *report* si affrettano a precisare come anche i contatti sui *social network*, pur non equiparabili a quelli della vita reale, «quando concernono persone coinvolte nell'attività professionale del magistrato devono essere contenute ovvero evitate, allorché essi possano incidere sulla sua immagine di imparzialità»[57].

Il documento in parola, ancorché adottato con riferimento alla magistratura amministrativa, costituisce indubbiamente un'utile cartina al tornasole pure nel contesto processualpenalistico. Più in generale, non può dubitarsi del fatto che una volta ammesso l'utilizzo di tali strumenti anche in capo ai giudici – per le ragioni sopra indicate – è inevitabile che si possano verificare casi nei quali venga richiesto allo stesso di "accettare l'amicizia" di altri utenti, alcuni dei quali possono essere avvocati, indagati o presunte vittime. Né appare esigibile imporre al giudicante «*an obligation to disclose social media connections*», enucleando così una regola che obbliga il titolare del potere di *ius dicere* a rivelare tutti i propri contatti sul *web* con difensori iscritti all'albo, parti in causa e testimoni[58].

2.2 Campagne mediatiche sui *social network* e rimessione del processo: una diade problematica

Muovendo dall'assunto per cui il processo penale e i suoi protagonisti non si collocano in una sfera di cristallo «separata dal flusso microstorico quotidiano»[59], è compito del legislatore predisporre strumenti adeguati a tutelare la libertà di giudizio di quegli uomini chiamati a esercitare il potere d'*imperio* su altri uomini. Per tale ragione, qualora l'imparzialità del giudicante venga messa in dubbio con riguardo all'Ufficio nel suo complesso, le parti processuali possono reagire invocando l'applicazione dell'istituto della rimessione (artt. 45 ss. c.p.p.) che, attribuendo loro un vero e proprio diritto di rifiutare lo *judex suspectus*, produce uno spostamento del processo dalla sua sede primigenia, derogando così al canone cristallizzato all'art. 25, comma 2, Cost.

È in tale contesto che occorre chiedersi se e come le dichiarazioni espresse dalla collettività attraverso le piattaforme digitali di comunicazione, oltrepassando il limite fisiologico e costituzionalmente (nonché, convenzionalmente) garantito del diritto all'informazione sulle vicende giudiziarie[60], possano incidere sul principio di imparzialità, imponendo così una

[56] Cons. Stato, *Delibera sull'uso dei mezzi di comunicazione*, cit., punto n. 3.
[57] Cons. Stato, *Delibera sull'uso dei mezzi di comunicazione*, cit., punto n. 8.
[58] Come proposto, invece, da B.P. COOPER, *Judges and Social Media: Disclosure as Disinfectant*, in *Science & Technology Law Review*, 2017, p. 523.
[59] F. CORDERO, *Procedura penale*, Milano, 2012, p. 151.
[60] Si tratta di un corollario che deriva da una lettura congiunta dell'art. 21 Cost., nella parte in cui garantisce a tutti la libertà di manifestazione del pensiero, e dell'art. 111, comma 1, Cost., laddove stabilisce che «la giustizia è amministrata in nome del popolo». L'esigenza di informare la collettività sulle vicende giudiziarie

dislocazione del processo in una sede diversa rispetto a quella originaria. In altre parole, può una campagna mediatica realizzata dal *quivis de populo* sui *social network* condizionare l'imparzialità di un intero Ufficio giudicante?

Il tema, come si intuisce, non è affatto d'avanguardia.

Già con l'avvento della radio, della televisione e, in seguito, dei *talk show* la dottrina processualista è stata chiamata ad affrontare il fenomeno dei «giudizi televisivi»[61], individuando un punto di equilibrio tra l'esercizio imparziale della funzione giurisdizionale e la libertà di informazione. La comparsa dei *social network*, in questa direzione, sembrerebbe collocarsi, a prima vista, in perfetta linea di continuità con quanto già in atto.

Le cose, però, non stanno proprio in questi termini, dal momento che le piattaforme di *sharing* hanno assunto oggi una pervasività tale da rendere il timore di un pregiudizio al canone di imparzialità sempre più reale e consistente[62].

In effetti, le interazioni fra gli utenti del *web*, assenti nei tradizionali mezzi di comunicazione di massa (*web* 1.0[63]), consentono di esprimere opinioni in merito a ogni singola attività processuale, generando in tal modo una costante pressione sociale su chi è chiamato a giudicare. Commenti, *post* e *like* rappresentano la forma con la quale viene realizzato quel «social-giustizialismo espresso telematicamente»[64] che mira a screditare e denigrare i principi fondamentali del rito a favore di una "gestione collettiva" del processo. Si è venuta a delineare, in tal modo, una nuova tipologia di comunicazione giudiziaria non più affidata a soggetti professionali, tenuti al rispetto di regole morali e deontologiche (ancorché, troppo spesso, disattese), bensì governata dai cd. "leoni da tastiera", privi di qualunque limite narrativo o contenutistico.

Tutto ciò, a ben considerare, ha segnato il passaggio da un «*trial by newspaper*»[65], cioè un "processo radio-televisivo" nel quale il giudizio di colpevolezza o innocenza dell'imputato era rimesso alla "sapienza" del giornalista esperto, a un processo nel quale «tutto è socializzato, cioè pubblicato e condiviso»[66] direttamente dalla collettività, senza l'intermediazione di terzi. In questo contesto, deve ritenersi ormai superata quell'idea di una «trasformazione della comunicazione in materia giudiziaria da una funzione informativa ad

è stata altresì ricondotta alla libertà di espressione garantita all'art. 10 CEDU (cfr., per tutte, Corte edu, 10 febbraio 1995, *Allenet de Ribemond c. Francia*).

[61] Definiti da M. CHIAVARIO, *L'impatto delle nuove tecnologie tra diritti umani e interessi sociali*, in *Dir. pen. proc.*, 1996, p. 143, come «la moda di chiamare il pubblico a pronunciarsi sulla colpevolezza di questo o quell'imputato», finendo così per «sostituir[si] alla funzione giudiziaria espressa da organi ufficialmente incaricati».

[62] Questo aspetto è sottolineato da R. ORLANDI, *La giustizia penale nel gioco di specchi dell'informazione*, in *Dir. pen. proc. – Riv. Trim.*, 2017, 3, p. 49: «anche più insidioso è l'uso dei *social media* nella circolazione di questo tipo di informazioni. Il carattere interattivo di codesti nuovi mezzi di comunicazione dà un'impressione di controllo democratico sull'informazione: impressione apparente (e fasulla), perché i *followers* che a quell'interazione partecipano tendono a costituirsi in gruppo preconcetto di pressione per diffondere notizie (spesso non verificate e persino infondate), fatte circolare al solo scopo di screditare qualcuno o di perseguire finalità politiche, più o meno esplicite».

[63] Sulle differenti caratteristiche del *web* 1.0 e del *web* 2.0, cfr. Parte I, Cap. I, par. 2.

[64] P. SAMMARCO, *Giustizia e* social media, Bologna, 2019, p. 33.

[65] G. GIOSTRA, *Processo penale e informazione*, Milano, 1989, p. 260.

[66] P. SAMMARCO, *Giustizia e* social media, cit., p. 54.

una formativa»[67]: gli abitanti del ciberspazio svolgono oggi una "funzione performativa", cioè volta direttamente alla "creazione" e alla successiva diffusione della notizia.

Sembra essersi al cospetto, dunque, di una nuova forma di "processo penale mediatico 2.0" che degrada le forme del rito a meri orpelli, a vantaggio di un circuito giudiziario parallelo che si risolve in un accertamento sommario dei fatti, in spregio delle più elementari garanzie. Ciò nonostante, la giurisprudenza di legittimità, come si vedrà a breve, non pare aver colto a pieno questo mutamento qualitativo, mostrando un atteggiamento particolarmente rigoroso che ha portato sovente al rigetto delle istanze di rimessione presentate dalla difesa.

Dal punto di vista normativo, come noto, la *translatio iudicii* richiede, ai sensi dell'art. 45 c.p.p., la sussistenza di determinati presupposti, ovverosia la presenza di gravi situazioni locali (*i*) tali da turbare lo svolgimento del processo (*ii*) e non altrimenti eliminabili (*iii*). La concorrenza di questi requisiti deve generare, alternativamente, un pregiudizio per la libera autodeterminazione dei soggetti che partecipano al processo (*a*) o per la sicurezza o l'incolumità pubblica (*b*) o, ancora, determinare motivi di legittimo sospetto (*c*).

Soffermando l'attenzione sui fenomeni di inquinamento mediatico in grado di pregiudicare il corretto esercizio della funzione giurisdizionale, assumono una specifica e diretta rilevanza i requisiti sub *i)* e *c)*. Nelle altre ipotesi (*a* e *b*), infatti, la campagna mediatica non assurge a presupposto indipendente dell'istanza di rimessione che, al contrario, è «autonomamente integrato dalle azioni di turbamento del processo rispetto alle quali la campagna mediatica rappresenta un irrilevante antecedente causale»[68].

Quanto al primo (*i*), la Suprema Corte, fin dalla pronuncia a Sezioni Unite resa nel caso Berlusconi[69], ha chiarito che «per grave situazione locale» deve intendersi un «fenomeno esterno alla dialettica processuale» riguardante l'ambiente territoriale nel quale il processo si svolge e connotato «da tale abnormità e consistenza da non poter essere interpretato se non nel senso di un pericolo concreto per la non imparzialità del giudice»[70].

In merito al secondo (*c*), poi, i giudici hanno ricondotto l'espressione *de qua* al «ragionevole dubbio che la gravità della situazione locale possa portare il giudice a non essere, comunque, imparziale o sereno, dovendo intendersi per imparzialità la neutralità, l'indifferenza del giudice rispetto al risultato, rispetto all'esito del processo»[71]. In questa prospettiva, perciò, i motivi di legittimo sospetto dovrebbero riferirsi a quelle situazioni nelle quali può emergere una realtà ambientale idonea a lasciar presagire un esito non imparziale

---

[67] G.P. VOENA, *Processo mediatico e "mass media": il passato e il presente*, in *Leg. pen.* web, 19 ottobre 2020, p. 159.

[68] A. PULVIRENTI, *Campagne mediatiche e istanze di rimessione del processo*, in N. Triggiani (a cura di), *Informazione e giustizia penale. Dalla cronaca giudiziaria al processo mediatico*, Bari, 2022, p. 246.

[69] Cass. pen., Sez. Un., 27 gennaio 2003, Berlusconi.

[70] Cass. pen., Sez. II, 23 dicembre 2016, n. 55328; Cass. pen., Sez. VI, 1° marzo 2016, n. 17170. Se ne ricava, anzitutto, l'irrilevanza, ai fini dell'accoglimento dell'istanza di rimessione, del «"clima" in cui si celebra il processo determinato dalle stesse condotte degli imputati», giacché, altrimenti, «si affiderebbe alla patologica (e talvolta anche illecita condotta delle parti processuali) lo strumento per poter "scegliere" fori alternativi rispetto a quello naturalmente determinato», così, da ultimo, Cass. pen., Sez. V, 25 gennaio 2022, n. 9432.

[71] Cass. pen., Sez. Un., 27 gennaio 2003, Berlusconi, cit.

del processo, senza che l'istante sia chiamato a dimostrare il concreto pregiudizio arrecato all'imparzialità, come accade, invece, nelle restanti ipotesi previste dalla norma[72].

A differenza di quanto fino ad oggi riscontrato con riguardo all'istituto della ricusazione, la giurisprudenza di legittimità ha avuto modo di soffermarsi sulla valenza dei *social network* ai fini della fondatezza di una istanza di rimessione del processo[73]. In tutti i casi oggetto di studio, la Suprema corte ha giustificato il rigetto delle istanze alla luce di una duplice argomentazione.

Per un verso, la presenza di commenti sui *social network* e di campagne mediatiche pressanti e caratterizzate da toni spesso esasperati risultano all'evidenza irrilevanti allorquando occorre valutare la sussistenza del primo requisito previsto all'art. 45, comma 1, c.p.p., nella parte in cui si richiede la presenza di gravi situazioni «locali» tali da turbare lo svolgimento del processo e non altrimenti eliminabili[74]. Nella nuova realtà iperconnessa, è agevole comprendere come anche un ipotetico spostamento della sede naturale non potrebbe comunque eliminare «l'eccezionale clamore mediatico nazionale né l'interesse dell'opinione pubblica da esso alimentato, sicché ogni ufficio giudiziario verrebbe a trovarsi in una situazione di potenziale condizionamento»[75].

Per altro verso, la giurisprudenza, mostrando di discostarsi dal tenore letterale del dato normativo, esclude, *de facto*, che i meri commenti, certamente discutibili, presenti nelle piattaforme digitali, siano in grado di alterare la situazione locale al punto da influire sul processo in corso[76]. Così facendo, però, i giudici sembrano subordinare «la dimostrazione della fondatezza di un pericolo alla prova di un danno concretamente realizzatosi»[77]. In questo modo, quella "presunzione relativa d'inidoneità"[78] della campagna di stampa a mettere in pericolo il bene protetto dalla rimessione si trasforma in una *probatio diabolica*: appare assai arduo dimostrare, in concreto, la negativa incidenza causale sul sereno esercizio della funzione giudiziaria ad opera «dei commenti proliferati sui *social network*, aperti ai contributi di una pluralità di persone dislocate in varie parti del territorio nazionale»[79].

Ciò nonostante, deve escludersi con fermezza che una campagna mediatica realizzata attraverso le piattaforme di *sharing* possa legittimare, di per sé, l'accoglimento di un'istanza di rimessione. Il connotato di «gravità» cui allude l'art. 45 c.p.p., infatti, non consente di identificare la situazione territoriale perturbatrice con un vago e generico «contesto ambientale massmediatico involgente l'ufficio giudiziario»[80]. Diversamente opinando,

[72] Ad avviso di A. PULVIRENTI, *Campagne mediatiche e istanze di rimessione del processo*, cit., p. 239 s., l'art. 45 c.p.p. ingloba, in realtà, due diverse fattispecie: quella di "pericolo concreto", riferibile ai motivi di legittimo sospetto, e quella di "evento", concernente le restanti ipotesi in cui la norma richiede il verificarsi di un vero e proprio pregiudizio.

[73] Cass. pen., Sez. I, 11 giugno 2018, n. 41990; Cass. pen., Sez. I, 22 novembre 2011, n. 47732.

[74] Cass. pen., Sez. I, 12 ottobre 2011, n. 4175; Cass. pen., Sez. I, 11 giugno 2018, n. 41990: «non sussiste, innanzitutto, nella specie, il necessario presupposto della "grave situazione locale", che i richiedenti ancorano, in primo luogo, alla "campagna di giustizialismo sfociata in diverse manifestazioni collettive, oltre che nell'ambito dei più comuni *social network*"».

[75] Cass. pen., Sez. I, 12 ottobre 2011, Misseri.

[76] Cass. pen., Sez. I, 1° dicembre 2016, n. 8788.

[77] A. PULVIRENTI, *Campagne mediatiche e istanze di rimessione del processo*, cit., p. 249.

[78] Così, G. MANTOVANI, *Informazione, giustizia penale e diritti della persona*, cit., p. 284, 291.

[79] Cass. pen., Sez. I, 22 novembre 2011, n. 47732, cit.

[80] Cass. pen., Sez. VI, 1° marzo 2016, n. 17170.

infatti, si finirebbe per erodere completamente la libertà di manifestazione del pensiero tutelata all'art. 21 Cost. Ammettere l'idoneità di una pur violenta campagna di stampa a influire sulla determinazione della competenza del giudice, peraltro, significherebbe consentire a chiunque sia in grado di controllare o condizionare gli organi di informazione – e, di riflesso, le campagne mediatiche – di distrarre il processo dalla propria sede naturale[81].

Epperò, da altra prospettiva, appare eccessivamente *tranchant* l'argomentazione spesa dalla Cassazione secondo cui il «debordare non commendevole della cosiddetta giustizia spettacolo», anche nei *social network*, ha finito per diventare fenomeno talmente normale che nessuno ci fa più caso. Seguendo questa linea di pensiero, la Corte sostiene che il giudicante, attorniato quotidianamente da notizie e dibattiti sui processi in corso, sarebbe perfettamente in grado, anche in ragione di non meglio precisate «qualità morali, psicologiche e di esperienza»[82], di gestire l'impatto emotivo della pressione mediatica, senza farsene condizionare. In tal modo, si giunge a negare, in radice, qualunque possibile incidenza sul valore dell'imparzialità tutelato all'art. 111, comma 2, Cost.

Di questa convinzione pare lecito dubitare, non foss'altro perché, come ha osservato autorevole dottrina, lo stereotipo del «giudice "corazzato" (per le sue qualità morali, psicologiche e di esperienza) […] nasconde una aprioristica valutazione che si risolve in un vero e proprio negazionismo»[83]. Per di più, una tale considerazione non potrebbe essere spesa con altrettanta fermezza con riguardo ai giudici popolari, soggetti notoriamente non abituati al "bombardamento mediatico" cui sono sottoposti, ormai quotidianamente, i magistrati ordinari[84].

Nessuno dubita, peraltro, della bontà dell'assunto giurisprudenziale secondo cui il carattere eccezionale proprio dell'istituto della rimessione, implicando una deroga al principio costituzionale del giudice naturale precostituito per legge, comporta «la necessità di un'interpretazione restrittiva delle disposizioni che lo regolano»[85].

Ciò nondimeno, sembra esservi un caso in cui la pressione mediatica esercitata sull'intera sede territoriale giudicante può comunque giustificare l'accoglimento di un'istanza di *translatio iudicii*. Si pensi, in particolare, alle ipotesi di "reati a vittima diffusa" (come, ad esempio, i delitti ambientali o contro la salute pubblica) in grado di ingenerare una pressione (e, sovente, un'aspettativa) sociale sull'intera collettività, giudici compresi[86].

---

[81] Cass. pen., Sez. II, 23 dicembre 2016, Mancuso.

[82] Cass. pen., Sez. I, 9 gennaio 1996, Farassino, in *Dir. inf. e informatica*, 1996, p. 678.

[83] E. AMODIO, *Estetica della giustizia penale. Prassi*, media *e* fiction, Milano, 2016, p. 139.

[84] In realtà, attenta dottrina ha messo in luce come, pur accettando l'idea – che, per inciso, non trova unanimi consensi in letteratura – di una maggiore vulnerabilità dei giudici popolari rispetto alle informazioni diffusa in Rete, deve comunque riconoscersi che è lo stesso Costituente ad aver introdotto «"nel giudizio la sensibilità media della frazione della società in cui il reato si assume commesso"». Se ne ricava, dunque, che la Corte d'assise, «nella sua componente laica» non «"è costitutivamente un giudice imparziale"», così G. MANTOVANI, *Informazione, giustizia penale e diritti della persona*, cit., p. 295.

[85] Cass. pen., Sez. III, 12 maggio 2015, n. 23962.

[86] L'ipotesi è prospettata anche da A. PULVIRENTI, *Campagne mediatiche e istanze di rimessione del processo*, cit., p. 252, il quale giustifica l'operatività della rimessione osservando come «così facendo, rimarrebbe sì inalterata la "forza comunicativa" della campagna mediatica […], ma si annullerebbe (o quantomeno si attenuerebbe) la sua "forza d'impatto" su chi deve giudicare».

Al di là di queste (remote) evenienze, la sensazione complessiva è quella di trovarsi al cospetto di un istituto, la rimessione del processo, che non è in grado di arginare un fenomeno di portata dirompente[87]. Uno «strumento quasi sempre imbelle»[88] che mostra tutta la sua inadeguatezza a fronte di una realtà sociale decisamente diversa da quella immaginata e cristallizzata dai *conditores* dell'88.

3. Piattaforme digitali e libertà personale: dal "diritto di accesso" a *Internet* al "diritto all'utilizzo" dei *social network*

Si è detto, a più riprese, che i *social network* rappresentano un imprescindibile strumento di comunicazione che, sfruttando le potenzialità della Rete, consente di sviluppare e intrattenere relazioni interpersonali con altri esseri umani. Da questo punto di vista, pertanto, è agevole comprendere il ruolo di cruciale importanza che assume l'accesso a *Internet* nell'ottica di un pieno sviluppo della personalità umana (art. 3, comma 2, Cost.). È solo garantendo a chiunque (cittadino e straniero) una connessione stabile e adeguata che può davvero assicurarsi una moderna ed effettiva partecipazione e inclusione sociale in quella che è stata plasticamente definita l'«era dell'accesso»[89].

Non stupisce, in questo contesto, l'insorgere di un dibattito, specialmente fra gli studiosi di diritto costituzionale, in merito al riconoscimento di un vero e proprio "diritto di accesso alla Rete"[90]. Oggetto di discussione è tanto la natura di questo "nuovo" diritto, quanto la necessità di un suo esplicito riconoscimento nella Carta Fondamentale.

Secondo alcuni Autori[91], la possibilità di fruire di un servizio di interconnessione globale sarebbe funzionale all'esercizio di altri diritti quali, ad esempio, la libertà di espressione e di manifestazione del pensiero. L'accesso a *Internet*, in questa prospettiva, assume il carattere di un diritto-mezzo o, meglio, di un «meta-diritto»[92], ovverosia una precondizione priva di una propria autonomia, ma indispensabile per assicurare il godimento di altre prerogative costituzionali, specialmente quelle attinenti alle libertà partecipative.

Epperò, l'idea di una "libertà cibernetica" come diritto servente, a sé stante rispetto alle singole garanzie costituzionali, non ha convinto altra parte della dottrina. Del resto – si è osservato – la navigazione in *Internet*, nell'attuale panorama socioeconomico, si configura

---

[87] Proprio la circostanza che nessun giudice possa dirsi immune e impermeabile al clima massmediatico ha indotto parte della dottrina a dubitare, nell'attuale contesto storico, della effettiva capacità dell'istituto in esame di far fronte alle pressioni mediatiche esercitate sui giudicanti. In tal senso, v. G. MANTOVANI, *Informazione, giustizia penale e diritti della persona*, cit., p. 267-271; R. ORLANDI, *La giustizia penale nel gioco di specchi dell'informazione*, cit., p. 49; G.P. VOENA, *Processo mediatico e "mass media"*, cit., p. 162.

[88] Così lo definisce, rispetto all'ipotizzata applicazione con riguardo ai casi di processo mediatico, G. GIOSTRA, *La giustizia penale nello specchio deformante della cronaca giudiziaria*, in *Riv. dir. Media*, 2018, 3, p. 28.

[89] J. RIFKIN, *L'era dell'accesso, La rivoluzione della* new economy, Milano, 2000.

[90] Per una panoramica sull'argomento, si rinvia a T.E. FROSINI, *Il diritto costituzionale di accesso ad* Internet, in M. Pietrangelo (a cura di), *Il diritto di accesso ad* Internet, Napoli, 2011, p. 23 ss.

[91] In tal senso, v., per tutti, O. POLLICINO, *The Right To Internet Access*, in A. von Arnauld – K. von der Decken – M. Susi (a cura di), *The Cambridge Handbook of New Human Rights*, Cambridge, 2020, p. 263 ss.

[92] Impiega tale locuzione, pur con riguardo al diritto all'assistenza linguistica (diritto all'interpretazione e alla traduzione), M. GIALUZ, *L'assistenza linguistica nel processo penale. Un meta-diritto fondamentale tra paradigma europeo e prassi italiana*, Padova, 2018, p. 139, per sottolinearne il carattere «funzionalmente prioritario – sia in termini concettuali che temporali – rispetto a ogni altra garanzia».

come «estrinsecazione della personalità del singolo, la quale ormai (e sempre di più) conosce una dimensione virtuale che si somma a quella naturale»[93].

Con riguardo, poi, all'individuazione di una idonea base giuridica del diritto in questione, la dottrina più accreditata[94] ha sottolineato come, pur in assenza di un'esplicita menzione a livello costituzionale, il suo fondamento possa essere ricavato da un'interpretazione sistematica ed evolutiva degli artt. 2, 3, 15 e 21 Cost. Da questo punto di vista, l'idea di inserire in Costituzione una previsione specifica e puntuale in materia – pur sostenuta da autorevoli autori e da plurime commissioni di studio[95] – sarebbe probabilmente foriera di non poche difficoltà esegetiche, poiché finirebbe con il cristallizzare una situazione che è, in realtà, in costante mutamento. Per di più, se si considera necessario il ricorso alla costituzionalizzazione di questo "nuovo" diritto, si finisce per sostenere implicitamente che la Carta delle Leggi non è idonea a tutelare libertà ulteriori rispetto a quelle esplicitamente garantite[96]. Una posizione, quest'ultima, sulla quale appare ragionevole esprimere più di qualche perplessità.

Ad ogni modo, e al netto delle tesi che si intendano prediligere, un dato appare incontestabile: il riconoscimento del diritto di accesso alla Rete alla stregua di una libertà fondamentale tutelata a livello costituzionale impone di interrogarsi in merito all'*an* e al *quomodo* di una sua eventuale limitazione per finalità processuali. La questione assume una certa consistenza tanto con riguardo alla fase investigativa come, ad esempio, nel caso di un sequestro preventivo di una pagina *social*, quanto, per quel che ora interessa, in relazione alla possibilità di restringere o escludere l'accesso ai "profili digitali" in sede di applicazione di una misura cautelare. Il carattere inviolabile del diritto, difatti, impone di valutare con particolare rigore e cautela ogni ipotesi volta a limitarne il concreto godimento.

3.1 Misure cautelari e *social webpages*: il divieto di avvicinamento ai luoghi frequentati dalla persona offesa (art. 282-*ter* c.p.p.)

Posto, dunque, che il diritto di accesso alla Rete finalizzato all'utilizzo delle piattaforme di comunicazione appare, secondo l'impostazione dominante, una libertà meritevole di pieno riconoscimento (ancorché in via mediata) a livello costituzionale, occorre rilevare come talune attività procedimentali siano in grado di comprimere, più o meno intensamente, siffatto diritto.

Il problema si pone, come anticipato, con riguardo al tema delle misure cautelari personali che limitano, direttamente o indirettamente, l'utilizzo della Rete.

---

[93] P. PASSAGLIA, Internet *nella Costituzione italiana: considerazioni introduttive*, in *Consultaonline.it*, 4 dicembre 2013, p. 19.

[94] P. PASSAGLIA, Internet *nella Costituzione italiana*, cit., p. 18; M. BASSINI, Internet *e libertà di espressione. Prospettive costituzionali e sovranazionali*, Roma, 2019, p. 93.

[95] Si ricordano, ad esempio, l'iniziativa di Stefano Rodotà volta a introdurre un nuovo art. 21-*bis* Cost., nonché il Disegno di legge costituzionale S. 1561 concernente l'introduzione dell'articolo 34-*bis* della Costituzione, recante disposizioni volte al riconoscimento del diritto di accesso a *Internet*, presentato al Senato il 1° luglio 2014.

[96] Per questa argomentazione, v. M. BASSINI, Internet *e libertà di espressione*, cit., 91.

La prima ipotesi che corre alla mente è quella del divieto di avvicinamento ai luoghi abitualmente frequentati dalla persona offesa *ex* art. 282-*ter* c.p.p.[97]. A tal proposito, ancorché non constino, allo stato attuale, precedenti giurisprudenziali specifici, viene scontato chiedersi se la disposizione possa o meno trovare applicazione anche con riguardo ai luoghi virtuali e, più nello specifico, ai siti di *social network*.

Sul punto, non è fuor d'opera sottolineare come tali interrogativi si siano manifestati pure in altri ordinamenti.

Nel sistema nordamericano, ad esempio, è prevista la possibilità per il giudice di adottare un *restraining* o un *protective order* a favore della vittima, con il quale si fa divieto all'indagato di intrattenere con quest'ultima qualsiasi contatto. Ricorrendo a un'interpretazione estensiva del dettato codicistico, la giurisprudenza d'oltreoceano ha stabilito che le interazioni su *Facebook*, *Twitter* e gli altri *social network* sono potenzialmente atti a violare un ordine restrittivo emesso dal Tribunale, tanto nel caso di interazioni *one-to-one*, quanto nelle ipotesi di apposizione di *like* o *tag*[98]. Parimenti, la giurisprudenza spagnola ha adottato un'esegesi evolutiva dei concetti di «*lugar*» e «*comunicación*» cui si riferisce l'art. 544-*bis* c.p.p., nel quale viene disciplinata una "misura cautelare di protezione" nei confronti delle vittime di delitti comuni[99].

Sul versante nazionale, l'art. 282-*ter* c.p.p. sembra porre un duplice ordine di problemi: occorre stabilire, da un lato, se il concetto di "luogo determinato" possa essere interpretato in modo tale da includervi anche il ciberspazio; dall'altro, se le interazioni sui *social network* rappresentino forme di "comunicazione", come tali vietate ai sensi del terzo comma della disposizione in parola.

Quanto al primo, deve condividersi la tesi – elaborata in dottrina con riguardo alla nozione di "domicilio informatico" – che equipara la Rete a un vero e proprio "luogo" inteso, alternativamente, come «spazio potenzialmente idoneo a contenere qualcosa» o «spazio virtuale generato dai dati», a nulla rilevando, dunque, l'immaterialità e l'aterritorialità del *cyberspace*[100].

Ciò nonostante, sembra potersi dubitare della legittima applicabilità della misura *de qua* in maniera tale da vietare *tout court* l'utilizzo del/dei *social network* in quanto luogo/luoghi abitualmente frequentati dalla persona offesa.

E si spiega.

Chiamato a dirimere un contrasto giurisprudenziale, il Supremo consesso, nella sua più autorevole composizione, ha stabilito che il giudice debba determinare specificamente i

---

[97] Identico è il caso della misura cautelare prevista all'art. 282-*bis*, comma 2, c.p.p., ove il giudice prescriva espressamente all'imputato di non avvicinarsi ai luoghi abitualmente frequentati dalla vittima. Lo stesso problema, invero, si pone anche con riguardo alla misura precautelare di cui all'art. 384-*bis* c.p.p.

[98] Per un'analisi di questi temi, si rinvia a T.A. HOFFMEISTER, *Liking the Social Media Revolution*, in *Science & Technology Law Review*, 2017, p. 517 s.

[99] Diverse sono, invece, le due misure di protezione *ad hoc* previste all'art. 544-*ter* c.p.p. dirette, rispettivamente, alla tutela delle vittime di violenza domestica («*protecciòn specìfica*») e di genere («*protecciòn renforzada*»).

[100] Cfr., rispettivamente, S. SIGNORATO, *Le indagini digitali*, cit., p. 59 e A. PAPA, *Espressone e diffusione del pensiero in* Internet. *Tutela dei diritti e progresso tecnologico*, Torino, 2009, p. 35. L'argomentazione verrà ripresa più approfonditamente nella Parte II, Cap. I.

luoghi oggetto del divieto di avvicinamento. A sostegno di tale condivisibile interpretazione muove sia un dato di natura testuale (ovvero, il riferimento espresso ai «luoghi determinati»), sia il fatto che le limitazioni poste all'indagato «risulterebbero, altrimenti, eccessivamente gravose rispetto ai suoi diritti di libertà e locomozione», assoggettando quest'ultimo a «compressioni della propria libertà personale di carattere indefinito»[101]. Senza considerare, in aggiunta, che, diversamente opinando, si finirebbe per imporre una condotta di astensione da un *facere* la cui individuazione sarebbe rimessa, di fatto, alla persona offesa.

Tali considerazioni, a ben vedere, possono essere estese anche all'ipotesi in esame.

Un divieto generalizzato di utilizzo delle piattaforme digitali, infatti, costituirebbe una misura eccessivamente gravosa per l'indagato, in quanto limitativa di quel diritto di accesso alla Rete costituzionalmente tutelato e finalizzato a garantire la stabilità delle relazioni interpersonali di un individuo, nonché l'esercizio delle libertà sociali da esso dipendenti. Si tratta di una considerazione che, peraltro, sembra trovare conforto nel disposto dell'art. 277 c.p.p., a mente del quale l'applicazione della misura cautelare deve salvaguardare quei diritti della persona a essa sottoposta, il cui esercizio, alla luce di un criterio di adeguatezza[102], non sia incompatibile con le esigenze cautelari indicate all'art. 274 c.p.p.

Per converso, parrebbe legittimo un provvedimento cautelare volto a inibire l'impiego delle piattaforme di *data sharing* solamente con riguardo a determinati "gruppi chiusi" o *chat* ai quali prende parte, abitualmente e in maniera attiva, la persona offesa, purché, come detto, essi vengano esplicitamente individuati dal giudice. È a quest'ultimo, in altre parole, che deve essere attribuito il compito di valutare, caso per caso, quali luoghi *online* siano interdetti alla presenza dell'indagato evitando, però, che «vengano imposte inibizioni che ne alter[i]no profondamente le elementari abitudini di vita al solo fine di assicurare abitudini voluttuarie della vittima»[103].

Dal punto di vista interpretativo, e in una prospettiva de *lege lata*, non può, tuttavia, ignorarsi una circostanza affatto dirimente.

Per quanto, come detto, appaia condivisibile l'adozione di un'"interpretazione 2.0" del concetto di "luogo", non può fare a meno di rilevarsi come un'eventuale restrizione dell'accesso ai *social network*, ancorché circoscritta a quei "luoghi virtuali" abitualmente frequentati dalla persona offesa, richieda, in sostanza, di ricorrere a un'esegesi estensiva di una disposizione limitativa della libertà personale; disposizione che, data la natura inviolabile del diritto in gioco (art. 13, comma 1, Cost.), dovrebbe essere oggetto esclusivamente di ermeneusi restrittive. Sarebbe auspicabile, dunque, un intervento

[101] Cass. pen., Sez. Un., 29 aprile 2021, n. 39005.

[102] V. BONINI, *Il sistema di protezione della vittima e i suoi riflessi sulla libertà personale*, Milano, 2018, p. 291.

[103] Nuovamente, V. BONINI, *Il sistema di protezione della vittima*, cit., p. 291. Parrebbe eccessivo, ad esempio, costringere l'indagato ad abbandonare gruppi *social* con centinaia o migliaia di persone per il solo fatto che gli stessi sono abitualmente "frequentati" dalla vittima, particolarmente attiva, ad esempio, con commenti o apposizione di *like* ai *post ivi* pubblicati.

legislativo volto a esplicitare la natura digitale e informatica dei luoghi di cui all'art. 282-*ter*, comma 1, c.p.p.[104].

In una diversa, ma connessa, prospettiva, si colloca, come anticipato, la *quaestio iuris* relativa al terzo comma della citata disposizione, a mente del quale il giudice può altresì vietare all'indagato di «comunicare, attraverso qualsiasi mezzo» con la persona offesa (ovvero, con i prossimi congiunti o con le persone legate a questa da rapporti affettivi).

Al netto dell'estrema genericità – se non totale carenza – dei presupposti che legittimano questa compressione della libertà di comunicazione[105], preme qui sottolineare come l'irrilevanza attribuita al mezzo[106] e l'impiego di una formula omnicomprensiva non lasci margini interpretativi circa la possibilità di ricondurre nella fattispecie anche le moderne piattaforme di *sharing* come, ad esempio, *Whatsapp* o *Facebook Messanger*. Nessun dubbio, perciò, che sia lo scambio di messaggi *one-to-one*, sia la pubblicazione di un *post* pubblico, ma con relativo *tag* o "menzione" (@nome dell'utente), rientrino a pieno titolo tra le condotte interdette all'indagato. Pure in quest'ultima circostanza, infatti, sembra potersi individuare un vero e proprio comportamento virtuale comunicativo univocamente diretto nei confronti del soggetto protetto dalla misura.

Più complesso è, invece, stabilire se le altre forme di interazione sui *social network* possano o meno essere ricondotte nel concetto di "comunicazione" cui allude la disposizione in esame. Si pensi, ad esempio, all'inserimento da parte dell'indagato di uno "stato" di *WhatsApp*[107] o alla semplice pubblicazione sulla propria pagina *Facebook* di un *post* visualizzabile da chiunque.

L'interrogativo non è di poco momento, giacché la violazione della prescrizione, come noto, può comportare la sostituzione o il cumulo della misura con altra più grave (art. 276, comma 1, c.p.p.), nonché l'integrazione del reato di cui all'art. 387-*bis* c.p., volto a punire, per l'appunto, la condotta di chi, essendovi legalmente sottoposto, violi gli obblighi o i divieti derivanti dal provvedimento applicativo delle misure di cui agli artt. 282-*bis* e 282-*ter* c.p.p.

---

[104] Il legislatore, però, non sembra essersi reso conto di tale esigenza. Nella recente novella – volta a contrastare il fenomeno della violenza sulle donne e della violenza domestica – che ha interessato la disposizione in parola, infatti, nulla è stato precisato a tal riguardo (l. 24 novembre 2023, n. 168).

[105] A fronte di una *littera legis* che omette qualsiasi richiamo a parametri predeterminati (come, ad esempio, la condotta concretamente tenuta dall'indagato), la dottrina ha comunque ancorato la possibilità di limitare lo *ius comunicandi* solo a fronte della sussistenza di una o più delle esigenze cautelati previste all'art. 274 c.p.p., ricavando, *a contrario*, un divieto di disporre la misura *de qua* con la generica finalità di tutelare la serenità psicologica della persona offesa. In tal senso, v., per tutti, V. BONINI, *Il sistema di protezione della vittima*, cit., p. 307, alla quale si rinvia per un esame più dettagliato della questione. Muovendo da tale considerazione, peraltro, l'A. soggiunge come la disposizione, così per come formulata, «non si presta a essere piegata duttilmente verso un impiego che limiti in modo più ampio e generalizzato i diritti comunicativi dell'imputato, neppure se questi si traducano in messaggi denigratori o derisori della persona della vittima su piattaforme *social*» (p. 310).

[106] L'irrilevanza dello strumento comunicativo ai fini dell'individuazione del campo di operatività della misura appare certamente condivisibile, per di più a fronte del continuo proliferare di nuove strumentazioni tecnologiche di "contatto sociale".

[107] Trattasi di una funzionalità che consente all'utente di condividere con la propria rubrica, per un tempo di ventiquattro ore, fotografie o testi scritti.

Fermo restando che, qualora il messaggio veicolato abbia carattere denigratorio od offensivo, potranno essere ritenuti sussistenti gli estremi del delitto di diffamazione, non v'è dubbio che entrambi i contenuti poc'anzi menzionati siano teoricamente visualizzabili dalla vittima. A quest'ultima, però, non sembra potersi imporre alcun obbligo negativo di *non facere* come, ad esempio, "bloccare il contatto *social*"[108] riferibile alla persona sottoposta a indagini. Si tratterebbe, peraltro, di un'operazione che non risulta sempre tecnicamente possibile, come nel caso del *social network* denominato *Google+*, le cui funzionalità non consentono di limitare a valle gli utenti abilitati alla visione dei propri contenuti.

Quid iuris, dunque, nell'ipotesi in cui la persona offesa giunga direttamente a conoscenza del messaggio?

In questi casi, a ben riflettere, non si è al cospetto di una condotta comunicativa esplicitamente indirizzata alla vittima: il fatto che i messaggi *online* possano essere letti da tutti gli iscritti alla piattaforma non può far presumere che l'indagato abbia una diretta e consapevole intenzione di comunicare con la persona offesa. Diversamente argomentando, si giungerebbe a enucleare un vero e proprio "divieto generalizzato di interagire sulle piattaforme *social* teoricamente frequentabili dalla vittima"; una preclusione che, a differenza di quanto stabilito per gli arresti domiciliari (art. 284, comma 2 c.p.p.), eccede dal novero delle prescrizioni accessorie stabilite dall'art. 282-*ter* c.p.p., né, tantomeno, appare in linea con il principio di adeguatezza e proposizionali delle misure cautelari.

A diverse conclusioni, tuttavia, potrebbe giungersi qualora il messaggio veicolato alla propria rete di contatti contenga riferimenti più o meno espliciti alla vittima. In detta evenienza, infatti, sembrano sussistere tanto un *corpus comunicandi*, quanto un *animus comunicandi*, giacché il messaggio, pur diffuso alla generalità degli utenti, è comunque indirizzato a un soggetto determinato. Si è al cospetto, a ben riflettere, di una volontà di comunicare attuata in modo indiretto, nel tentativo di aggirare il divieto imposto dal provvedimento giurisdizionale. Per tale ragione, ciò che rileva, alla luce di un criterio teleologico, è che quelle parole, una volta contestualizzate, siano rivolte a un destinatario rispetto al quale vige un divieto di comunicazione.

Alle medesime conclusioni dovrebbe giungersi anche nel diverso caso in cui la persona offesa pubblichi un messaggio come "stato" di *Whatsapp* o un *post* sulla propria bacheca di *Facebook* e questi siano successivamente visualizzati dal soggetto sottoposto alla misura. Al pari dell'apposizione di un *like*, pure la semplice visualizzazione, difatti, è in grado di veicolare un messaggio dal contenuto comunicativo – che sarà ricevuto dalla vittima sul proprio *device* – paragonabile all'invio da parte dell'imputato di una dichiarazione con la seguente dicitura: "ho visto il tuo *status*".

3.2 S*ocial network* e arresti domiciliari tra "funzione conoscitiva" e "attività comunicative"

Con il provvedimento che dispone gli arresti domiciliari, il giudice, qualora lo ritenga necessario, può specificare nell'ordinanza applicativa divieti o limiti per la persona ristretta a comunicare con soggetti diversi da quelli che coabitano con lui o che lo assistono (art. 284,

[108] Il termine allude alla possibilità di escludere un determinato soggetto dalle proprie interazioni digitali.

comma 2, c.p.p.). La *ratio* di questa «prescrizione dotata di specifica ed aggiuntiva efficacia afflittiva»[109] rispetto al semplice obbligo di abitazione forzata è, all'evidenza, quella di evitare il pericolo che il soggetto ristretto possa pregiudicare le esigenze di acquisizione probatoria o commettere ulteriori reati.

In quanto previsione accessoria, il divieto di comunicare consente di adeguare l'intervento coercitivo alla situazione concreta, di talché ogni limitazione alla libertà garantita all'art. 15 Cost. deve costituire oggetto di specifica motivazione da parte del giudice, sia sotto il profilo della necessità, sia della sussistenza di specifiche esigenze processuali[110].

Oggetto di attenzione, in questa sede, è se sia lecito l'utilizzo dei *social network* per chi si trovi ai domiciliari cd. "ristretti", cioè con limiti o divieti imposti alla facoltà di comunicare.

A differenza di quanto osservato con riguardo alla misura di cui all'art. 282-*ter* c.p.p., la Suprema corte ha già avuto modo di soffermarsi, ancorché con un approccio non sistematico e organico, sul rapporto tra le nuove piattaforme di *sharing* e la previsione contenuta nell'art. 284 c.p.p.

L'elaborazione giurisprudenziale muove da un assunto certamente condivisibile. Come già la Commissione europea ebbe a sottolineare nel 1996[111], una delle caratteristiche uniche di *Internet* è l'ibridazione dei servizi messi a disposizione degli internauti: strumento per comunicare e, simultaneamente, per conoscere. Si giunge, così, a sostenere che l'impiego di *Internet* non possa essere vietato *tout court* ove non rappresenti il mezzo per intrattenere comunicazioni con terzi, bensì «abbia solamente una funzione conoscitiva o di ricerca»[112]. Una limitazione tal fatta, del resto, darebbe luogo a una totale soppressione dei diritti e delle facoltà spettanti a ogni singolo individuo (*in primis*, la libertà di informazione e il diritto di accesso alla Rete), consentendo l'impiego di modalità esecutive che, incidendo sulla qualità della misura, finirebbero per snaturarla, rendendola diversa da quella disciplinata dal legislatore ed equiparandola di fatto alla detenzione intramuraria.

Preso atto, dunque, delle proteiformi funzionalità che connotano le moderne piattaforme *web* (*rectius*, informative e comunicative), dovrebbe ritenersi legittimo un utilizzo "passivo" dei profili *social* in uso all'indagato con la finalità, ad esempio, di raccogliere informazioni, visualizzare contenuti o tenersi aggiornato sull'evoluzione della vita pubblica locale o nazionale. Accogliendo questa prospettiva, peraltro, dovrebbe escludersi con forza ogni automatismo cautelare diretto a giustificare la sostituzione *in peius* della misura in ragione della mera connessione al *social*, in assenza di un accertamento circa la realizzazione da parte dell'indagato di una vera e propria attività comunicativa[113].

---

[109] Così, Cass. pen., Sez. I, 8 settembre 2020, n. 6934.

[110] È orientata in questo senso anche la giurisprudenza di legittimità: cfr., *ex plurimis*, Cass. pen., Sez. IV, 7 marzo 2017, n. 20380.

[111] COMMISSIONE EUROPEA, *Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni. Informazioni di contenuti illegale e nocivo su* Internet COM(96)487, 16 ottobre 1996.

[112] Cass. pen., Sez. II, 29 settembre 2010, n. 37151.

[113] La giurisprudenza, del resto, ha affermato che l'eventuale violazione del divieto stabilito all'art. 284, comma 2, c.p.p. «non può essere desunta in via presuntiva dall'acclarato utilizzo della navigazione informatica da parte dell'indagato, ma deve essere oggetto di specifica motivazione da parte del G.I.P. che ha disposto, a fronte della presunta violazione, la sostituzione della misura con altra più grave» (Cass. pen., Sez. II, 29 settembre 2010, n. 37151, cit.).

A quest'ultimo proposito, risulta parimenti convincente l'esegesi estensiva ed evolutiva adottata dalla giurisprudenza, volta a includere nel concetto di "comunicazione" previsto all'art. 284, comma 2, c.p.p. anche quella realizzata tramite le piattaforme di *social network*. È ben vero – si dirà – che la disposizione in esame, a differenza di quanto previsto all'art. 282-*ter* c.p.p., non impiega espressioni generali e omnicomprensive («attraverso qualsiasi mezzo») tali da includere pure la trasmissione di dati *online*. Ciò nonostante, parrebbe irragionevole escludere questi nuovi sistemi dal novero degli strumenti che, pur diversi dalla parola, sono in grado di veicolare un contenuto conoscitivo. Per tale ragione, dunque, è corretto sostenere che il divieto di comunicare «deve intendersi esteso, pur in assenza di prescrizioni dettagliate e specifiche, anche alle comunicazioni sia vocali che scritte attraverso *Internet*»[114] e le altre piattaforme di *social network*[115]. In altre parole, qualora il giudice non indichi nel dettaglio i singoli mezzi di comunicazione dei quali è vietato l'utilizzo, deve ritenersi implicita un'ostatività di carattere generale, comprensiva delle strumentazioni *social*.

Da quanto detto consegue che si devono considerare ricomprese nel divieto (o nelle limitazioni *ad hoc* imposte dal giudice), altresì, le comunicazioni realizzate mediante le piattaforme di messaggistica istantanea – quali, ad esempio, *Whatsapp* o *Messanger* – che siano dirette a uno specifico soggetto o a una platea determinata di individui.

Al contrario, non sembrerebbe censurabile, in linea generale, il comportamento "attivo" dell'indagato che si limiti a pubblicare un *post* o un *tweet* con la propria cerchia di contatti. Il primo capoverso della disposizione in esame, come detto, consente al giudice di limitare o vietare esclusivamente condotte *stricto sensu* "comunicative"; un concetto, quest'ultimo, che, come insegna la miglior dottrina[116], richiede il carattere dell'inter-subiettività, cioè, il fatto che lo scambio informativo sia diretto a uno o più soggetti determinati. Ed è proprio tale criterio, del resto, che consente di distinguere la libertà di comunicazione, tutelata all'art. 15 Cost., da quella libertà di «comunicazione circolare […] del pensiero»[117] garantita all'art. 21 Cost. In quest'ordine di idee, perciò, la mera condivisione di un'opinione o un convincimento con la propria cerchia di contatti non può ritenersi ricompresa, *de lege lata*, nel divieto stabilito all'art. 284, comma 2, c.p.p.

Sennonché, vi possono essere casi nei quali questa conclusione deve essere rimeditata.

Si allude, in particolare, all'ipotesi – non dissimile da quella già considerata con riguardo all'art. 282-*ter* c.p.p. – in cui l'utilizzo di messaggi diffusi indistintamente ai propri *followers* celi, in realtà, un contributo comunicativo *ad personam*, cioè, indirizzato a uno specifico soggetto. Nell'esaminare una fattispecie del tutto assimilabile a quella considerata, la Suprema corte ha recentemente confermato il provvedimento del Tribunale del riesame che aveva disposto l'aggravamento della misura custodiale da domiciliare a inframuraria a

[114] In questi termini, Cass. pen., Sez. I, 24 marzo 2017, n. 54109, par. 2.2.

[115] Esplicitamente, Cass. pen., Sez. IV, 6 dicembre 2011, n. 4064, ove, nel rigettare la tesi prospettata dalla difesa secondo cui la prescrizione *ex* art. 284, comma 2, c.p.p. avrebbe dovuto richiamare esplicitamente anche le comunicazioni "a distanza", afferma che «il divieto di comunicare con terze persone […] vale anche per le comunicazioni tramite *Internet* sul sito *Facebook*».

[116] P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, p. 163.

[117] Testualmente, ancora, P. BARILE, *Dritti dell'uomo e libertà fondamentali*, cit., p. 163.

seguito della condivisione di un messaggio (nel caso di specie, si trattava, in realtà, di un *repost*) sul profilo *social* dell'indagato[118].

Dalla lettura della (stringata) motivazione è possibile ricavare un criterio generale utile a guidare l'interprete nello studio di casi analoghi.

Occorre distinguere, in particolare, la mera diffusione di un messaggio con la propria Rete di contatti dalla pubblicazione di un *quid* informativo che, parimenti divulgato a terzi, risulta, però, «oggettivamente criptico» in quanto «indirizzato a chi può comprendere perché sottintende qualcosa di riservato e conosciuto da una ristretta cerchia di persone»[119]. In quest'ultima circostanza, l'impiego della propria bacheca virtuale assume solo apparentemente finalità conoscitive o divulgative, celando, in realtà, un intento velatamente comunicativo. In tali evenienze, dunque, si può ritenere che il soggetto sottoposto alla misura meriti un aggravamento del suo *status libertatis*: egli, con la propria condotta, ha realizzato una sorta di "elusione" del dettato normativo, in spregio alla *ratio essendi* della disposizione.

Sul punto, una notazione appare quantomai opportuna: dovrà essere il giudice, ancora una volta, a valutare, caso per caso mediante un'attenta ricostruzione della *voluntas comunicandi* dell'indagato, se quel comportamento divulgativo astrattamente riconducibile nell'alveo dell'art. 21 Cost. rappresenti, in realtà, un modo per aggirare il divieto imposto dal provvedimento cautelare.

4. La metamorfosi del "sapere" processuale: le informazioni presenti nelle *web communities* quale "petrolio digitale" per le autorità investigative

La produzione massiva e bulimica di informazioni rappresenta la più grande innovazione apportata dai *social network* nella società del XXI secolo. Difficile contestare, in effetti, l'assunto secondo cui le piattaforme digitali sono ormai divenute la più grande "banca dati" del mondo; in esse circolano, ogni istante, miliardi di notizie connotate dai più variegati contenuti. In un contesto nel quale, come ha ricordato la stessa Corte di cassazione, la «vita [delle persone è] scandita dai nuovi strumenti di comunicazione»[120], il continuo e inarrestabile progresso tecnologico che sta alla base del loro funzionamento consente di generare informazioni sempre più "consistenti", sia sotto il profilo quantitativo che qualitativo.

In realtà, non si può fare a meno di osservare come agli albori dell'era di *Internet*, le informazioni prodotte dai primi *personal computer* fossero legate essenzialmente a esigenze di ricerca nel settore scientifico. Con il passare del tempo, però, la diffusione di massa di siffatte strumentazioni – *in primis*, in numerosi settori delle attività lavorative – ha reso gli stessi *computer*, prima, i *tablet* e gli *smartphone*, poi, veri e propri mezzi di interazione nella vita sociale di ogni singolo cittadino[121].

---

[118] Cass. pen., Sez. II, 14 luglio 2016, n. 46874.

[119] Cass. pen., Sez. II, 14 luglio 2016, n. 46874, cit.

[120] Cass. pen., Sez. IV, 9 febbraio 2017, n. 11428, par. 3.

[121] Strumentazioni, non a caso, comunemente definite come propaggini elettroniche dell'essere umano. È divenuto celebre, in tal senso, quanto affermato dalla Corte Suprema americana nel caso *Riley c. California*, 573 U.S. 373, 25 giugno 2014: «*modern cell phones are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy*». Di

Questa trasformazione ha avuto ripercussioni anche sulla tipologia di dati prodotti: da semplici *file* contenenti numeri ai più poco comprensibili, passando per documenti aziendali, fino ad arrivare – e questo è il punto fondamentale – a una produzione costante e ininterrotta di informazioni relative a ogni singola attività compiuta dagli individui nella loro quotidianità[122]. Attraverso la rivoluzionaria triade – *Internet*, *Mobile* e *social network* –, l'individuo ha avuto accesso a una dimensione spazio-temporale fatta di simboli, valori e comportamenti. La tendenza, nell'ambito della *web society*, è quella di una condivisione delle proprie informazioni personali in ambienti (erroneamente) percepiti come privati[123] ("il profilo", la "bacheca", la "*chat*"); il che, peraltro, rende impossibile un controllo effettivo su detti contenuti nel momento in cui vengono condivisi con terzi.

A fronte di tale scenario, lo studioso del processo penale non può certo rimanere indifferente, non foss'altro perché il buon funzionamento degli ingranaggi del rito criminale dipende, in larga misura, dalla quantità e dalla qualità delle informazioni di cui può disporre chi è chiamato a esercitare il potere di *ius dicere*.

Sotto tale profilo, è affermazione ricorrente quella per cui il procedimento penale, al pari di ogni serie cronologicamente ordinata di atti, è funzionale al perseguimento di un uno o più specifici obiettivi. Occorre essere ben consapevoli, tuttavia, della molteplicità ed eterogeneità degli scopi sovente attribuiti a quest'ultimo a seconda del contesto storico di riferimento[124]. Il rito, infatti, si configura come uno strumento multifunzionale: opera come mezzo di difesa sociale[125] e attua la repressione criminale ripristinando l'ordine sociale turbato dal delitto[126]; funge da veicolo per proteggere l'indagato dagli abusi del potere pubblico[127]; e si configura come uno strumento di garanzia della presunzione di

un'«"appendice della persona" e dell'io più profondo» parlano P. TONINI – C. CONTI, *Il diritto delle prove penali*, Milano, 2014, p. 482.

[122] Rileva questo aspetto anche A. SCALFATI, *Un ciclo giudiziario "travolgente"*, in *Proc. pen. giust.*, 2016, p. 114, per il quale «*Internet* e gli strumenti digitali hanno radicalmente mutato il modo di essere degli individui, permettendo sviluppi dell'identità umana impensabili fino a poco fa; persino le relazioni, individuali e di gruppo, hanno cambiato volto, generando archivi privati dalle proporzioni straordinarie».

[123] Accreditate ricerche empiriche dimostrano come circa il 75/80% degli utenti dei *social network* considerino "private" le attività realizzate nelle piattaforme digitali con "amici" o "gruppi di amici" (C.S. SCOTT-HAYWARD – H.F. FRADELLA – R.G. FISCHER, *Does Privacy Require Secrecy? Societal Expecttions of Privacy in the Digital Age*, in *American Journal of Crime Law*, 2015, p. 20 ss., e, spec., p. 54).

[124] Come ricordano, da ultimo, M. GIALUZ – J. DELLA TORRE, *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022, p. 5. Si veda, in tal senso, l'*excursus* storico-giuridico offerto da G. SABATINI, *Principi di diritto processuale penale*, vol. I, Catania, 1948, p. 29 ss.

[125] Per tutti, E. FERRI, *I nuovi orizzonti del diritto e della procedura penale*, Bologna, 1881, p. 110.

[126] V. MANZINI, *Trattato di diritto processuale penale italiano*, vol. I, Torino, 1925, p. 140-142. In questo senso, E. FLORIAN, *Principi di diritto processuale penale*, Torino, 1932, p. 52, nt. 1, richiama l'efficace definizione del processo come semplice «mezzo in servigio degli scopi della tutela penale».

[127] È nota la definizione di "procedura penale" offerta dal Carrara: strumento per la «salvaguardia dei galantuomini» (F. CARRARA, *Il diritto penale e la procedura penale. Prolusione al corso accademico di diritto penale dell'anno 1873-1874*, Lucca, 1873, p. 15).

innocenza[128]. L'eterogeneità dei fini assegnati[129], dunque, varia al mutare delle «forme» che lo contraddistinguono, «cioè dei sistemi con cui [esso] viene organizzato»[130].

A prescindere dalla tesi che si intenda prediligere[131], il processo penale pare, in ogni caso, connotato da un'intrinseca "vocazione conoscitiva", a fronte della quale l'informazione è assunta a «fattore di conoscenza che rende possibile l'elaborazione di decisioni giudiziali»[132]. Al fine di perseguire lo scopo cui esso è preordinato, il giudice penale è chiamato a confrontarsi con un evento del passato, come tale storicamente esaurito[133]. E, dunque, se l'obiettivo ultimo del rito non può che essere identificato nella ricostruzione di un fatto storico, il giudicante, dovendo indagare su «"dati" preesistenti»[134], finisce per assumere (anche) le vesti dello storico, pur con le numerose differenze che intercorrono tra le due figure[135].

---

[128] Questa è la tesi sostenuta, ad es., da O. MAZZA, *Le persone pericolose (in difesa della presunzione d'innocenza)*, in *Dir. pen. cont*., 20 aprile 2012, p. 1 ss. *Contra*, icasticamente, V. MANZINI, *Trattato di diritto processuale penale italiano*, cit., p. 141: «la moderna democrazia, grossolana e confusionaria in tutto, ha avuto anche qui il torto di intorbidire i concetti, affermando che lo scopo del processo penale è quello principalmente di tutelare l'innocenza, o che questo fine è uguale a quello della repressione».

[129] Si considerino, altresì, quelle teorie che identificano lo scopo del processo con la "ricerca della verità". Cfr. M. TARUFFO, *La semplice verità. Il giudice e la costruzione dei fatti*, Bari, 2009, p. 83. Si pensi, ancora, all'idea di un processo penale come luogo «diretto a massimizzare lo scopo della risoluzione dei conflitti», come sostenuto da M.R. DAMAŠKA, *I due volti della giustizia e del potere. Analisi comparatistica del processo*, Bologna, 1991, p. 212.

[130] Così, G. SABATINI, *Principi di diritto processuale penale*, cit., p. 29, per il quale il processo penale non rappresenta né uno strumento nelle mani del pubblico potere, finalizzato ad attuale la repressione, né un mezzo a tutela dell'innocenza (presunta) dei cittadini: il fine ultimo del rito «è assai più vasto, e dalla sua precisa determinazione scaturisce la nozione integrale del processo penale moderno».

[131] Tra le molte, sembra potersi condividere l'impostazione autorevolmente adottata da G.D. PISAPIA, *Introduzione*, in AA.VV., *Il codice di procedura penale. Esperienze, valutazioni, prospettive*, Milano, 1994, p. 26, secondo cui il processo penale «è, per sua stessa natura, un complesso di garanzie per la corretta applicazione delle norme penali sostanziali». È solo muovendo da tale postulato, prosegue l'A., che può affermarsi «che un codice di procedura penale può anche essere, indirettamente, uno strumento di difesa sociale, ma solo nel senso che riesca a funzionare in modo tale da assicurare che i colpevoli siano puniti nel più breve tempo possibile (ed a maggior ragione siano assolti gli innocenti)» (p. 27). La stessa visione è prospettata, in termini sostanzialmente speculari, da V. GREVI, *Garanzie individuali ed esigenze di difesa sociale nel processo penale*, in L. Lanfranchi (a cura di), *Garanzie costituzionali e diritti fondamentali*, Roma, 1997, p. 261 s.; ID., *Ambiguità e limiti dell'uso del processo per fini di difesa sociale*, in G. Riccio (a cura di), *Dalle indagini preliminari alla sentenza di primo grado*, Napoli, 1979, p. 224; E. AMODIO, *Garantismo e difesa sociale nel nuovo rito accusatorio*, in G. Riccio (a cura di), *Dalle indagini preliminari alla sentenza di primo grado*, cit., p. 243 s.

[132] Così, R. ORLANDI, *Il processo nell'era di* internet, in *Dir. pen. proc*., 1998, p. 140.

[133] G. CAPOGRASSI, *Giudizio, processo, scienza, verità*, in *Riv. dir. proc*., 1950, p. 1. Dei processi penali come «macchine retrospettive miranti a stabilire se qualcosa sia avvenuto e chi l'abbia commesso» parla F. CORDERO, *Procedura penale*, cit., p. 568.

[134] Così, P. CALAMANDREI, *Il giudice e lo storico*, in *Riv. dir. proc*., 1939, p. 105.

[135] Sui rapporti tra il giudice e lo storico (nonché sulle relative analogie e differenze), imprescindibile, oltre al già citato P. CALAMANDREI, *Il giudice e lo storico*, cit., p. 105 ss., M. TARUFFO, *Il giudice e lo storico: considerazioni metodologiche*, in *Riv. dir. proc*., 1967, p. 444 ss.

In questa prospettiva, il rito si mostra nella sua essenza più intima: un "vorace" fruitore di dati[136], una macchina che «si "nutre" di informazioni»[137], la cui ricerca diviene lo "scopo mediato" del processo, passaggio necessario e indispensabile per il perseguimento degli obiettivi che a esso vengono di volta in volta attribuiti[138].

Questa impostazione, come noto, è stata impropriamente manipolata dalla Corte costituzionale nelle numerose pronunce che, nella metà degli anni '90, hanno contribuito all'enucleazione del "principio di non dispersione della prova", intimamente legato all'identificazione della «ricerca della verità» materiale[139] quale «fine primario ed ineludibile del processo penale»[140]. È evidente, in quella sede, l'approccio finalistico adottato dai giudici della Consulta: l'assunto in base al quale il processo penale deve pervenire a una ricostruzione dei fatti il più possibile aderente alla realtà materiale giustifica – ad avviso dei giudici – l'apprensione di una quantità illimitati di informazioni, anche in spregio dei principi fondanti il modello accusatorio (oralità e contraddittorio). La fallacia di tale argomentazione non è tanto nell'aver qualificato la "ricerca della verità" quale valore irrinunciabile del modello accusatorio[141], quanto nell'irrilevanza attribuita al metodo di accertamento e ai limiti epistemologici dello stesso. L'idea che il processo penale debba essere investito di un «compito di ricerca della verità "ad ogni costo"»[142] e, cioè, a

[136] Del processo penale come «recettore di dati» parla L. LUPÁRIA, Privacy, *diritto della persona e processo penale*, in *Riv. dir. proc.*, 2019, p. 1455. Parimenti, S. CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate istituzionali*, in D. Negri (a cura di), *Protezione dei dati e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 5, la quale si riferisce al rito criminale come uno strumento di raccolta, selezione e raffronto di informazioni.

[137] R. ORLANDI, *Il processo nell'era di* internet, cit., p. 140.

[138] A considerazioni differenti non dovrebbe giungersi neppure accogliendo l'idea di un rito indifferente alla teoretica degli scopi (F. CORDERO, *Procedura penale*, cit., p. 101). La concezione del processo come un «modello ideologicamente neutro», ovverosia quale «pura operazione tecnica», indifferente ai possibili esiti del medesimo, infatti, non farebbe venir meno la vocazione conoscitiva che lo contraddistingue. Quest'ultima, benché svincolata da un fine prestabilito, costituirebbe comunque un momento essenziale per la concreta applicazione delle norme processuali.

[139] Come ricorda, ad es., J. FERRER BELTRAN, *Prova e verità nel diritto*, Bologna, 2004, p. 71, la distinzione tra i concetti di "verità materiale" e "verità processuale" è stata proposta sul finire del XIX secolo dalla dottrina tedesca, per poi essere sottoposta a censure nella prima metà del '900. Sull'essenziale infondatezza di tale concettualizzazione, imprescindibile, P. CALAMANDREI, *Verità e verosimiglianza nel processo civile*, in *Riv. dir. proc.*, 1955, p. 165, che ricollega la "verità" di un fatto al «massimo grado di verosimiglianza che, in relazione ai limitati mezzi di conoscenza di cui il giudicante dispone, basta a dargli la certezza soggettiva che quel fatto è avvenuto». Cfr., già, G. BRUGNOLI, *Della certezza e prova penale*, Modena, 1846, p. 3: «*allorchè parliam di certezza nei criminali Giudizj, non abbiamo scordar che siam uomini, e che l'imperfezione nostra ci accompagna sempre in qualsiasi umana istituzione*».

[140] Testualmente, Corte cost., 18 maggio 1992, n. 255. In questa direzione si collocano le ulteriori, "sventurate" e ben note sentenze della Corte costituzionale che hanno interpolato il contenuto degli artt. 195, 500 e 513 c.p.p. (cfr., rispettivamente, Corte cost., 22 gennaio 1992, n. 24; Corte cost., 18 maggio 1992, n. 254; Corte cost., 2 novembre 1998, n. 361).

[141] Secondo accreditate ricostruzioni, infatti, l'idea di una scissione tra il concetto di verità e i valori fondanti il modello processuale accusatorio «è un errore capitale di cui approfittano i nemici del contraddittorio» (P. FERRUA, *Studi sul processo penale*, vol. III, Torino, 1992, p. 22, nt. 27).

[142] M. CHIAVARIO, *Il processo penale dopo la nuova decretazione "d'emergenza": ancora una volta alla ricerca di una bussola*, in *Leg. pen*., 1993, p. 343, ove l'Autore pone in discussione, perlomeno in termini dubitativi, la scelta dei *Conditores* del "nuovo" codice di espungere qualunque riferimento nell'ordito legislativo al concetto di "verità" quale scopo del processo penale.

prescindere dalle modalità di accertamento, è il frutto di un grossolano errore concettuale: nel processo penale «la caccia [non] vale più della preda»[143].

Preso atto di tati distorsioni interpretative, è agevole constatare, in ogni caso, come "l'istanza conoscitiva" della Procedura, pur sempre immutata nel tempo, abbia modificato il proprio oggetto. Negli ultimi decenni, infatti, si è assistito a una lenta metamorfosi della fonte conoscitiva del rito: dalla testimonianza orale al *bit* digitale.

Per rendersene conto è sufficiente scorrere le disposizioni contenute nel Capo III del Titolo II del Libro IV del codice: le norme in tema di istruzione dibattimentale sono perlopiù dedicate alla disciplina della prova dichiarativa, ovverosia la *regina probatorum* del sistema penale accusatorio[144]. Nelle intenzioni dei *conditores*, l'esame dibattimentale delle fonti orali, in linea di continuità con l'opinione tradizionale[145], incarnava il metodo per eccellenza di formazione della prova, poiché diretta manifestazione della regola del contraddittorio; quest'ultimo, rappresentava (e rappresenta ancora oggi) «il migliore strumento, o, se si preferisce, il meno imperfetto, per la ricerca della verità»[146]. Quale metodo di raccolta e confronto tra visioni contrapposte, il canone previsto all'art. 111, comma 3, Cost. trova la propria linfa vitale proprio nella dialettica tra le parti: la *cross examination*, esprimeva (ed esprime tutt'ora) in modo inequivocabile l'adesione a un modello accusatorio[147], nel quale la maieutica è posta a fondamento della concezione argomentativa della prova.

Lo sviluppo di *Internet*, tuttavia, ha, almeno in parte[148], scardinato questo modello.

Non è un mistero, del resto, che la macchina giudiziaria muti la propria fisionomia «attraverso i nuovi strumenti del conoscere [tra i quali debbono essere annoverate le nuove tecniche informatiche] almeno altrettanto che attraverso le riscritture interne alla scienza del diritto»[149].

---

[143] F. CORDERO, *Ideologie del processo penale*, Milano, 1966, p. 220.

[144] L'espressione, come noto, è mutuata dal valore probatorio che nei sistemi inquisitori – e, prima ancora, presso il popolo Ebraico e gli antichi romani – veniva riconosciuto all'istituto della confessione.

[145] Plasticamente rappresentata dalle parole del Florian, per il quale «nel quadro delle prove, la prova testimoniale è quella cui sempre il processo penale attinse il più copiosamente: la testimonianza è il modo più ovvio di ricordare e ricostruire gli avvenimenti umani, è la prova in cui l'indagine giudiziaria si esplica con maggiore energia. Di essa non si può fare a meno» (E. FLORIAN, *Delle prove penali*, vol. II, Milano, 1924, p. 62).

[146] O. MAZZA, *Il garantismo al tempo del giusto processo*, cit., p. 5. Una verità che, precisa l'A., non è certamente «quella illusoria verità oggettiva, umanamente irraggiungibile […], ma della verità giudiziale che è direttamente influenzata e condizionata dal metodo di indagine prescelto». Nello stesso senso, v. G. UBERTIS, *Sisifo e Penelope. Il nuovo codice di procedura penale dal progetto preliminare alla ricostruzione del sistema*, Torino, 1993, p. 268, ove si afferma che il contraddittorio rappresenta il miglior metodo «escogitato dagli uomini per stabilire la verità di enunciati fattuali, in qualsiasi campo e specialmente in quello giudiziario».

[147] L. FERRAJOLI, *Diritto e ragione. Teoria del garantismo penale*, Roma-Bari, 2004, p. 576, sottolinea come si possa «chiamare accusatorio» solo quel modello che configura «il giudizio come una contesa paritetica […] ingaggiata con la difesa mediante un contraddittorio pubblico ed orale».

[148] La crisi della prova dichiarativa, in realtà, è da ricondurre anche ai recenti studi in tema di psicologia della testimonianza che evidenziano come la memoria del testimone sia un qualcosa di estremamente "fragile", tutt'altro che infallibile e, di conseguenza, non così affidabile come tradizionalmente sostenuto.

[149] Così, nel cogliere lo stretto legame tra *novum* digitale e innovazione processuale, G. ALESSI, *Il processo penale. Profilo storico*, Roma-Bari, 2007, p. 180.

In realtà, l'ingenuo convincimento dei Padri del «codice "analogico" del 1988»[150] emerse già con la comparsa della prova scientifica nel panorama processuale. Le nuove tecniche di accertamento, in grado di dimostrare – con un grado di certezza più o meno variabile[151] – la correlazione tra una determinata condotta e il susseguente evento, hanno difatti scardinato un modello processuale che sino ad allora guardava con sospetto all'ingresso di modelli scientifici nella dialettica processuale[152].

Con il passare del tempo, dunque, la "prova per testimoni" (che, nelle more dei vecchi codici, ricopriva sovente un ruolo decisivo in qualsivoglia istruzione dibattimentale) ha man mano perso la sua centralità, sia a livello pratico-applicativo che a livello dogmatico, lasciando il posto all'avvento di una prova informatico-digitale[153]. È ormai tramontata l'epoca in cui, per dirla con le parole del Florian, la *declaratio* rappresentava il modo più appropriato e scientificamente affidabile per ricostruire *ex post* le vicende umane, giacché le «manifestazioni della delinquenza» erano, «d'ordinario, ben lungi dal prestarsi a modi precostituiti di prova»[154]. Le moderne tecnologie, per contro, sono oggi in grado di cristallizzare con un semplice *click* tutti quegli eventi del passato di rilevanza processuale o, quantomeno, il materiale probatorio utile alla loro ricostruzione.

Di qui, l'ineludibile esigenza del pubblico ministero e della polizia giudiziaria di ricercare "materiale elettronico" ha provocato un radicale mutamento dei tratti «essenziali [del] metodo investigativo e, con esso, [del] "codice genetico" del sapere processuale»[155], tanto che non appare peregrino affermare come ad oggi l'apprensione di informazioni nel corso del processo penale avvenga essenzialmente attraverso i "cavi" che collegano i numerosi dispositivi elettronici di uso comune. Sembrano essersi avverate, dunque, le profezie di quell'acuta dottrina che, anni or sono, preconizzava l'avvento di un'epoca nella quale «qualsiasi tipo di fonte di prova [sarebbe stato] "digitale", in quanto il processo di informatizzazione e digitalizzazione della nostra società condizionerà direttamente il mondo giuridico e, soprattutto, il suo aspetto processuale»[156]. E non si dovrà rimanere stupiti

---

[150] Così descritto, onde evidenziare l'inadeguatezza del codice Vassalli rispetto alla tematica della digitalizzazione del processo, da B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Milano, 2022, p. 257.

[151] È stato da tempo messo in luce, in effetti, come il concetto di certezza esuli dal panorama processuale. Sul punto, v. F. STELLA, *Il giudice corpuscolano. La cultura delle prove*, Milano, 2005, p. 98, il quale sottolinea come «occorre prendere atto che nella scienza non vi sono certezze, né verità definitive e che l'idea della verità scientifica [e tecnologica] come verità certa è esattamente un mito, cioè una falsa storia. […] La storia della scienza, in altre parole, è un cimitero di errori». D'altro canto, già F.M. PAGANO, *La logica dei probabili. Per servire di teoria alle prove nei giudizi criminali*, Salerno, 1924, p. 6, sottolineava come «il regno della probabilità è confinante con quello della certezza, ma è diviso da quello».

[152] La fallacia di tale argomentazione è stata messa in luce da M.R. DAMAŠKA, *Il diritto delle prove alla deriva*, Bologna, 2003, p. 205, per il quale «un numero sempre più elevato di fatti rilevanti nel processo può essere oggetto di accertamento soltanto con strumenti tecnici sofisticati».

[153] Lo rilevano, tra gli altri, M. GIALUZ, *Premessa*, in Id. (a cura di), *Le nuove intercettazioni. Legge 28 febbraio 2020 n. 7*, in *Dir. Internet*, 2020, Suppl. al n. 3, p. 1, per il quale i nuovi strumenti di indagine tecnologica «hanno scalzato la testimonianza dal ruolo di regina *probationum*»; G. DI PAOLO, voce *Prova informatica* (dir. proc. pen.), in *Enc. dir.*, Annali VI, Milano, 2013, p. 736.

[154] E. FLORIAN, *Delle prove penali*, cit., p. 63.

[155] S. LORUSSO, *Investigazioni scientifiche, verità processuale ed etica degli esperti*, in *Dir. pen. proc.*, 2010, p. 1346.

[156] G. ZICCARDI, *Scienze forensi e tecnologie informatiche*, in L. Lupária – G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano,

qualora, negli anni a venire, dovesse rivelarsi veritiera anche l'affermazione di chi ha recentemente sostenuto come nel giro pochi lustri «*pràcticamente el cien por cien de los conflictos estaràn relacionado con algùn elemento tecnològico*»[157]. *Internet*, in conclusione, può essere senza dubbio definita come la più grande "fonte di prova" del XXI secolo[158].

Se queste sono le premesse, pare che l'avvento dei *social network sites* abbia ampliato notevolmente – e possa modificare, in senso ancor più incisivo – le capacità conoscitive del procedimento penale (e, specialmente, dell'inchiesta), ponendo nuovamente in luce la necessità di ri-valutare quel complesso bilanciamento tra l'interesse collettivo alla conoscenza (e al successivo accertamento) dei fatti e i diritti fondamentali degli individui[159]. Nella prospettiva adottata dal processualpenalista, infatti, le *social webpages* non sono semplici strumenti di comunicazione, bensì una «*digital goldmine*»[160] ricca di informazioni rilevanti per la ricostruzione del fatto di reato.

Il riflesso sulla fase investigativa è di immediata evidenza.

Il combinato congiunto tra i *big data* prodotti dalle interazioni fra gli utenti e lo sviluppo di strumentazioni tecnologiche sempre più sofisticate hanno generato nuove tecniche di indagine penale generalmente conosciute come *big data policing* o *big data mining*, ovverosia atti investigativi consistenti, come si è detto, in vere e proprie operazioni di raccolta e trattamento massivo di dati[161].

Se è vero che nel contesto dei *social network sites* l'esperienza acquista valore solo attraverso la condivise di informazioni[162] – e, pertanto, tali strumenti risultano ontologicamente orientati alla produzione di dati (specialmente per ragioni di *marketing*) – e, al contempo, il processo penale è assimilabile a un "raccoglitore" di informazioni, occorre, di conseguenza, individuare nuove garanzie processuali atte a evitare che le numerose "tracce" contenute nella "scatola nera digitale" siano oggetto di un'indiscriminata apprensione da parte del potere pubblico. In altre parole, se si condivide l'idea che le nuove piattaforme digitali costituiscono uno spazio inedito per lo «sviluppo della personalità umana», deve consequenzialmente affermarsi che «le incursioni investigative in quegli spazi

2007, p. 9. Il tema è stato in seguito ripreso e approfondito dall'A. in ID., *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni penali*, Milano, 2012, p. 296 ss.

[157] F. BUENO DE MATA, *Las digilencia de investigacion penal en la cuarta revolucion industrial. Principios teoricos y problemas practicos*, Cizur Menor, 2019, p. 21.

[158] In questi termini, J. DELGADO MARTIN, *Investigacion tecnologica y prueba digital en todas las jurisdicciones*, Madrid, 2018, p. 38. Anche M. TROGU, *Intrusioni segrete nel domicilio informatico*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 567, sottolinea come la rete *Internet* si stia rivelando «uno strumento attraverso il quale i soggetti processuali possono ricercare ed acquisire le fonti di prova con l'uso di strumenti sempre più sofisticati».

[159] In tal senso, benché sul versane dei riflessi del fenomeno giuridico dei *social network sites* nel diritto civile, si esprime anche C. PERLINGIERI, *Profili civilistici dei* social networks, Napoli, 2014, p. 23 s.

[160] Così, P. MURPHIY – A. FONTECILLA, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, in *Richmond Journal of Law & Technologiy*, 2013, p. 9.

[161] Da ultimo, mette in luce, in una prospettiva più generale, i rischi derivanti dall'analisi dei dati su larga scala, G. LASAGNI, *Dalla riforma dei tabulati a nuovi modelli di integrazione fra diritti di difesa e tutela della* privacy, in *Leg. pen.* web, 21 luglio 2022, p. 14.

[162] Si tratta del cd. *sharing*, ovverosia la condivisione di notizie in ambiente virtuale.

sono in grado di scalfire in misura e modi altrettanto inediti quel nucleo intimo dell'individuo che uno Stato democratico si impegna a riconoscere e rispettare come inviolabile»[163].

4.1 *Drafting* normativo: tecniche di legislazione applicate alle nuove indagini informatiche (anche nei *social network*)

«Si scrivono centinaia di libri su come si devono leggere e interpretare le norme giuridiche, ma nessuno su come andrebbero scritte»[164]. Con queste parole, autorevole dottrina ha plasticamente messo in rilievo uno degli aspetti maggiormente problematici relativi al rapporto tra il potere legislativo, le scelte di politica processuale e le nuove metodologie di indagine penale a contenuto tecnologico.

Ad uno sguardo attento, infatti, pare che l'impetuosa avanzata della modernità digitale abbia reso ogni tentativo di regolamentazione del fenomeno *de quo* assai complesso e, almeno in alcuni casi, del tutto vano. L'implementazione di strumenti investigativi "non analogici" sembrerebbe richiedere maggiore capacità di intervento da parte del legislatore, un onere al quale quest'ultimo, troppo spesso, non è in grado far fronte[165]. E, infatti, si assiste, con maggiore frequenza, a una sorta di "rincorsa disperata" alla normativizzazione della tecnologia "dell'ultimo minuto" che, tuttavia, non può dirsi il preludio per una disciplina efficace ed effettiva. In una "società liquida" nella quale «le situazioni in cui agiscono gli uomini si modificano prima che i loro modi di agire riescano a consolidarsi in abitudini e procedure»[166], non v'è da stupirsi, però, se anche il legislatore processuale fatichi a trovare la quadratura del cerchio.

Questa inerzia, peraltro, contribuisce, in maniera affatto limitata, a esasperare ancor di più quella componente "creativa" che ormai da anni connota l'operato della giurisprudenza di merito e di legittimità. Chiamati a risolvere problematiche concrete, i giudici, a fronte di un dettato normativo assente o estremamente lacunoso, si trovano "costretti" a adottare interpretazioni manifestamente *contra legem* o financo lesive dei diritti fondamentali dell'accusato. Onde rendersi conto di ciò, è sufficiente considerare il richiamo bulimico operato in sede pretoria alla fattispecie di cui all'art. 189 c.p.p., con l'obiettivo di colmare ogni *deficit* normativo e consentire l'ingresso alle nuove "tecniche di indagine 2.0"[167].

In considerazione di ciò, pertanto, è agevole comprendere l'importanza assunta dal *modus legiferandi* nella costruzione di un sistema giuridico in grado di cogliere le innovazioni apportate dall'evoluzione tecnologica.

Quando ci si appresta a esaminare, sotto tale profilo, il rapporto tra diritto e tecnologia, occorre muovere da una premessa che deve costituire la stella polare di ogni riflessione: qualsivoglia regolamentazione normativa, financo la più concisa, puntuale ed efficace, è

---

[163] Così, in una prospettiva più generale, R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen*., 2018, p. 538.

[164] F. CAPRIOLI, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, in L. Lupária – L. Marafioti – G. Paolozzi (a cura di), *Dimensione tecnologica e prova penale*, Torino, 2019, p. 52.

[165] Mette in luce, nel contesto in esame, l'inerzia del legislatore nel disciplinare repentinamente tale fenomeno, M. DANIELE, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. pen. giust*., 2018, p. 831 ss.

[166] Z. BAUMAN, *Vita liquida*, Bari, 2006, VII.

[167] Cfr. Parte II, Cap. II.

destinata a rimanere sempre un passo indietro rispetto alle conquiste del progresso tecnologico. Con ciò, occorre precisarlo, non vuol certo affermarsi che il giurista debba rinunciare alla ricerca di regole e principi in grado di governare l'inarrestabile flusso digitale. Un approccio di questo tipo, come ha osservato la dottrina più accreditata, svelerebbe, sul versante processuale, un atteggiamento arrendevole «un po' sospett[o]», celando, invero, «uno dei tanti pretesti per screditare ulteriormente la già screditatissima legalità processuale»[168].

Il punto della questione, casomai, sta nel *quomodo*: come deve reagire il sistema processuale per adattarsi al meglio ai nuovi artefatti investigativi che bussano alla porta del rito penale?

La stessa sfida, come si può intuire, coinvolge, più in generale, la scienza giuridica nel suo complesso.

Chiamato a confrontarsi con scenari inediti, lo studioso è posto dinnanzi all'alternativa tra interpretare le norme vigenti in modo da offrire risposte nuove ed efficaci; oppure, muoversi alla ricerca di costrutti normativi innovativi, sondando terreni sino ad allora inesplorati. Senza voler necessariamente ricondurre quanto appena descritto in quella che la dottrina ha definito la costante «dialettica fra "conservatori" e "innovatori"»[169], non pare sia possibile – e, anzi, risulti affatto auspicabile – schierarsi aprioristicamente a favore dell'uno o dell'altro approccio. Occorre, invece, distinguere a seconda del fenomeno preso in considerazione e del tipo di legislazione con la quale si è chiamati a interfacciarsi. Non appaiono condivisibili, dunque, sia le tesi volte a difendere strenuamente i principi classici della tradizione giuridica – «manifestazione di miopia [scientifica]»[170] –, sia quelle improntate a una rassegnazione a fronte di fenomeni prima ignoti e a un totale soverchiamento delle regole preesistenti.

Alla luce del quadro appena descritto, di due ordini sono le risposte che si offrono al quesito sul quale ci si interroga.

La prima consiste nel tipizzare, in maniera quanto più dettagliata possibile, i singoli strumenti investigativi, nell'intento di ricomprendere nell'ordito normativo tutte le funzionalità digitali che la tecnologia mette a disposizione. È evidente che, alla luce di quanto premesso poc'anzi, questa non possa essere la strada da intraprendere. Un approccio tal fatto, invero, si rivelerebbe in partenza fallimentare, dal momento che l'evoluzione tecnologica rischia di rendere obsolescenti e inadeguate le nuove disposizioni ancor prima della loro entrata in vigore[171]. Illusorio, dunque, tentare di imbrigliare la scienza in apparati normativi iper-dettagliati: l'approccio casistico, in tali circostanze, non è affatto consigliato.

---

[168] F. CAPRIOLI, *Tecnologia e prova penale*, cit., p. 52, da cui sono tratte le ultime due citazioni.

[169] R. ORLANDI, *Trasformazione dello Stato e crisi della giustizia penale*, in M. Vogliotti (a cura di), *Il tramonto della modernità giuridica. Un percorso interdisciplinare*, Torino, 2008, p. 235, per il quale «messo di fronte a fenomeni non riducibili alle classificazioni tradizionali, lo studioso ha una duplice scelta: o ravvisa in esse patologiche evasioni dal reticolo concettuale che domina l'ambito della realtà studiata; oppure intraprende una revisione delle categorie di comprensione, sforzandosi di includere quei fenomeni in un nuovo ordine concettuale».

[170] Così, nuovamente, R. ORLANDI, *Trasformazione dello Stato e crisi della giustizia penale*, cit., p. 235.

[171] In questo senso, v. G. DI CHIARA, *Atipicità e sistemi probatori: linee per una fenomenologia generale*, in V. Militello – A. Spena (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Torino, 2018, p. 376, per il quale questa linea esegetica evidenzia «non lievi controindicazioni, comportando tempi tecnici dilatati e

Per tali ragioni, una parte della dottrina ha prospettato la necessità di mutare il punto di osservazione del fenomeno *de quo*. Anziché tentare di disciplinare ogni possibile attività intrusiva posta in essere dalla "polizia giudiziaria digitale", si è auspicata l'introduzione di categorie probatorie generali che possano fungere da guida ogniqualvolta si tratti di limitare le garanzie fondamentali dei cittadini[172]. Si tratta, in buona sostanza, di nuove categorie investigativo-probatorie dalle quali sia possibile evincere i "casi" e i "modi" dell'ingerenza nella sfera privata dell'individuo. Alcuni Autori, peraltro, si sono spinti, sulla scia di tale impostazione, fino a sostenere che la riserva di legge costituzionale (artt. 13 ss. Cost.) non imporrebbe, in realtà, una «specifica previsione legislativa per ogni tipologia di strumento […] utilizzabile», dovendosi ritenere sufficiente l'individuazione delle «garanzie fondamentali che dovranno essere riconosciute all'indagato e ai terzi potenzialmente coinvolti»[173] dall'atto investigativo.

In questa direzione, si colloca, almeno in parte, la recente interpolazione normativa che ha interessato l'ordinamento iberico, un sistema al quale è opportuno riferirsi, come si avrà modo di osservare a più riprese, allorquando ci si interroghi sull'impiego di nuove metodologie di indagine penale.

La *Ley Oganica* n. 13/2015[174], preso atto della necessità di aggiornare il regime giuridico dei mezzi di ricerca della prova a fronte delle nuove tecnologie dell'informazione, ha introdotto un capitolo *ad hoc* nella *Ley de Enjuiciamiento Criminal* (artt. 588-*ter* a – 588-*septies* c) interamente dedicato alla «*regulación de las medidas de investigación tecnológica*». Lungi dal predisporre un ordito normativo avente natura squisitamente ed esclusivamente settoriale, il legislatore spagnolo ha scelto di introdurre disposizioni di carattere generale che, nel rispetto dei principi di specialità, idoneità, necessità e proporzionalità[175] hanno consentito al costrutto in parola, perlomeno fino ad oggi, di non essere sopraffatto dall'avanzamento tecnologico[176].

---

rischiando, d'altronde, di non essere in grado di tenere il passo rispetto al progredire continuo degli sviluppi tecnologici».

[172] A favore di tale approccio, v., pur con differenti sfumature, S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2015, p. 789 s.; F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., p. 57-62; W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Milano, 2021, p. 317 ss.

[173] È la tesi sostenuta, ad es., da G. LASAGNI, *L'uso di captatori informatici* (trojans) *nelle intercettazioni "fra presenti"*, in *Dir. pen. cont.*, 7 ottobre 2016, p. 11.

[174] Ley Organica 5 ottobre 2015, n. 13, avente ad oggetto la modifica della *Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*. Per una panoramica sui contenuti della legge, v. S. PEREIRA PUIGVERT, *Las medidas de investigación tecnológicas y su injerencia en la privacidad de las personas y la protección de datos personales*, in *Investigación y prueba en los procesos penales de España e Italia*, diretto da I. Villar Fuentes, Cizur Menor, 2019, p. 297 ss.

[175] L'enunciazione esplicita di tali principi con riguardo alle nuove metodologie di indagine tecnologica rappresenta una delle più marcate novità della riforma. Come ha osservato L. BACHMAIER WINTER, *Registro remoto de equipos informàticos y principio de proporcionalidad en la Ley Orgànica 13/2015*, in *Boletìn del Ministerio de Justicia*, 2016, p. 14, «*la novedad radica en que pro primera vez la LECRIM no solo menciona especìficamente esos requisitos, sino que ademàs ofrece una definicòn de los mismos y criterios para su interpretaciòn*».

[176] Questa è l'opinione espressa da uno dei massimi esperti di prova penale digitale nell'ordinamento iberico (F. BUENO DE MATA, *Las digilencia de investigacion penal en la cuarta revolucion industrial*, cit., p. 22; ID.,

L'approccio adottato dalla dottrina da ultimo richiamata e fatto proprio dal legislatore iberico merita di essere condiviso, ancorché con talune necessarie precisazioni.

Non può ragionevolmente dubitarsi del fatto che l'inarrestabile incedere del progresso digitale renda inopportuni interventi *ad hoc* diretti a una iper-normazione di dettaglio. D'altro canto, già agli albori dell'era degli elaboratori elettronici, autorevole dottrina, benché in una prospettiva non strettamente processuale, metteva in guardia dai possibili rischi che sarebbero potuti derivare dall'impiego di legislazioni "analitiche" basate su fattispecie chiuse: «in presenza di una realtà caratterizzata da una forte dinamica sociale e da una elevata innovazione tecnologica», si osservava, il ricorso a clausole generali quale tecnica ordinaria di normazione rappresenta «lo strument[o] più adeguat[o] a regolare una realtà dal dinamismo crescente e quindi irriducibile alla tipizzazione di ipotesi definite a priori»[177].

Sembra parimenti sconsigliabile, però, anche un'esaltazione del cd. principio di neutralità tecnica, cioè di una pretesa indifferenza della legislazione processuale rispetto alla tipologia di strumentazione investigativa di volta in volta adottata[178]. Pur condividendosi l'assunto secondo cui il *focus* dell'analisi deve essere incentrato non tanto sul singolo strumento di indagine, bensì sulle garanzie processuali da tutelare, va osservato come, talvolta, le caratteristiche e le funzionalità proprie dell'artefatto digitale finiscono per incidere sui diritti fondamentali dell'individuo in maniera tale da rendere vetusto quel bilanciamento tra esigenze investigative e libertà fissato dal legislatore all'interno del codice. In questi casi, a ben vedere, il *lawmaker* è chiamato a intervenire per aggiornare quell'assetto di interessi non più attuale.

Alla luce di ciò, pare che la configurazione più ragionevole si risolva in un *mix compositum* tra le due prospettazioni sopra ricordate[179]. Non una tipizzazione settoriale, né, tantomeno, un'unica disciplina generale e astratta, bensì una normativa organica che sappia cogliere, all'evenienza, se e come il nuovo strumento incida su quell'equilibrio – individuato a monte dal Parlamento – tra esigenze investigative e salvaguardia dei diritti fondamentali.

Investigación y prueba de delitos de odio en Redes Sociales: Técnicas OSINT e inteligencia policial, Valencia, 2023, p. 128).

[177] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, 1973 (Ristampa anastatica a cura di G. Alpa), Napoli, 2018, p. 147, da cui sono tratte le ultime due citazioni.

[178] Per una valorizzazione di tale principio, v. G. LASAGNI, *L'uso di captatori informatici*, cit., p. 11.

[179] Già S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit., p. 147, invitava a diffidare dall'idea per cui «alle clausole generali non possano essere accompagnate prescrizioni analitiche».

PARTE II

"RETI SOCIALI VIRTUALI" TRA PREVENZIONE E INVESTIGAZIONE

CAPITOLO I

ATTIVITÀ *LATO SENSU* INVESTIGATIVE E NUOVE DECLINAZIONI DEI DIRITTI FONDAMENTALI DELLA PERSONA NEI *SOCIAL WEBSITES*

SOMMARIO: 1. *Web investigations* tra garanzie fondamentali e legittime istanze di persecuzione penale: alla ricerca di un giusto equilibrio. – 2. Le libertà "di relazione" nel *web* 2.0: segretezza, riservatezza e intimità della vita privata. – 3. Nuove forme di comunicazione e interpretazioni evolutive dell'art. 15 Cost.: *Whatsapp*, *Telegram* e le altre piattaforme di messaggistica istantanea. – 4. Il cd. *data sharing* e il "naufragio" della *privacy* nei *social network*. – 5. Il domicilio informatico: vecchi diritti, nuove tutele.

1. *Web investigations* tra garanzie fondamentali e legittime istanze di persecuzione penale: alla ricerca di un giusto equilibrio

A seguito della violenta irruzione del fenomeno digitale nella vita quotidiana di ogni cittadino, i diritti di libertà tradizionalmente riconosciuti nelle Costituzioni novecentesche e nelle Carte sovranazionali (*rectius*, libertà personale, domiciliare, segretezza e riservatezza delle comunicazioni[1]), «si appalesano friabili, penetrabili, sottoponibili ad un "bombardamento tecnologico" in grado di annichilirli completamente»[2]. Per tale ragione, si va avvertendo sempre più la necessità di aggiornare le categorie giuridiche del costituzionalismo moderno, tanto che alcuni autori hanno messo in luce l'esigenza di andare "oltre il costituzionalismo" o, financo, di elaborare un «costituzionalismo digitale»[3]. A fronte di cambiamenti sociali epocali, del resto, la storia insegna che l'uomo sviluppa nuovi bisogni e, con essi, emerge la necessità di dar vita a prerogative e garanzie che, lungi spesso dal rappresentare nuovi diritti *stricto sensu* intesi, siano in grado di rispondere alle esigenze concrete di volta in volta in rilievo[4].

---

[1] Invero, si è osservato come la libertà di domicilio e quella di corrispondenza «integrano e specificano la sfera normativa dell'art. 13 Cost.: l'una garantendo alla persona un certo àmbito spaziale, l'altra garantendo una delle forme più dirette di collegamento della persona con il mondo esterno» (così, P. BARILE – E. CHELI, voce *Corrispondenza (libertà di)*, *Enc. dir.*, vol. X, Milano, 1962, p. 744).

[2] S. MARCOLINI, *Regole di esclusione costituzionali e nuove tecnologie*, in *Discrimen*, 2006, p. 389.

[3] È questa la tesi sostenuta da E. CHELI, *Conclusioni*, in *Osservatorio sulle fonti*, 2021, 2, p. 955: «sappiamo anche che il costituzionalismo ha attraversato varie stagioni: c'è stato il costituzionalismo settecentesco e ottocentesco dell'età liberale, il costituzionalismo novecentesco dello Stato sociale, il costituzionalismo garantista dello Stato costituzionale del secondo dopoguerra, ma oggi dobbiamo dare atto che quella che si qualifica come la quarta rivoluzione industriale legata ai processi di digitalizzazione - che stiamo vivendo – viene ad aprire la strada a una nuova stagione del costituzionalismo fondata su presupposti diversi da quelli del passato, stagione che potremmo qualificare del "costituzionalismo digitale». Di «nuovo costituzionalismo» nell'era digitale ha parlato anche S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, p. 7.

[4] Per tale ragione, non appare corretto parlare di "generazioni di diritti" (prima, seconda, terza, quarta etc.): «i diritti dell'uomo, pur fondamentali che siano, sono diritti storici, cioè nati in certe circostanze, contrassegnate da lotte per la difesa di nuove libertà contro vecchi poteri, gradualmente, non tutti in una volta e non una volta per sempre» (così, N. BOBBIO, *L'età dei diritti*, Torino, 1990, XIII). Si mostra parimenti scettico rispetto all'utilità delle «varie periodizzazioni delle diverse "generazioni"» dei diritti R. BIN, *Critica della teoria dei diritti*, Milano, 2018, p. 55.

Il timore per una lenta e silenziosa erosione dei diritti fondamentali non poteva non avere impatto anche sul versante del procedimento penale, notoriamente descritto – *in primis*, dalla dottrina tedesca (Sax) – in termini di "diritto costituzionale applicato"; formula con la quale si intende descrive un rapporto tra le due macroaree della scienza giuridica improntato non tanto a un'«affinità», bensì a una vera e propria «derivazione o discendenza» del primo rispetto al secondo[5]. D'altro canto, come autorevolmente osservato, la formula *de qua* è volta ad attribuire al rito criminale «il compito precipuo di garantire la dignità dell'imputato quale soggetto anch'esso titolare d'una sfera di diritti intoccabili dal pubblico potere»[6].

L'impatto delle *Information and Communication Technologies*, dunque, impone di chiedersi, sul versante processuale, se sia opportuno, nonché auspicabile, individuare *ex novo* ulteriori "diritti di libertà digitali" e/o declinare in maniera "2.0" le garanzie già previste nel dettato costituzionale[7]. Il quesito assume una certa consistenza se riferito alla fase *lato sensu* investigativa (*ante* e *post delictum*), giacché, a causa dell'impiego di strumenti ad alto contenuto tecnologico, qualsiasi attività di raccolta di dati informatici va tendenzialmente a comprimere uno o più diritti fondamentali della persona, tanto da indurre a chiedersi se questo mutamento qualitativo del *modus investigandi* non rappresenti un chiaro indice dell'avvento di un vera e propria nuova "procedura penale digitale"[8].

Con riferimento alle tecniche di indagine nei *social network*[9], peraltro, questo timore ha indotto gli studiosi d'oltreoceano a interrogarsi sulla necessità di redigere una vera e propria «*Social Network Constitution*»[10]. Con il fine di proteggere le libertà fondamentali dei

---

[5] È questa la lettura offerta da R. ORLANDI, *La prolusione di Rocco e le dottrine del processo penale*, in *Criminalia*, 2010, p. 223.

[6] Testualmente, D. NEGRI, *Diritto costituzionale applicato: destinazione e destino del processo penale*, in *Proc. pen. giust.*, 2019, p. 554. Secondo G. ILLUMINATI, *Costituzione e processo penale*, in *Giur.it.*, 2008, p. 522, la locuzione *de qua* allude al fatto che la funzione del rito penale – «anzi, la giustificazione stessa della sua esistenza — sia quella di garantire i diritti individuali, che nella Costituzione trovano il loro principale riconoscimento».

[7] R. ORLANDI, *Sicurezza e diritto penale. Dialogo di un processualista italiano con la scuola di Francoforte*, in M. Donini – M. Pavarini (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, p. 103; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 6. È questo, d'altro canto, il quesito al quale sono chiamati a rispondere, nella nuova realtà digitale, tanto i costituzionalisti, quanto gli altri studiosi del diritto: «le tecnologie determinano nuove forme di diritti di libertà oppure possono essere incardinate e quindi riconosciute nell'alveo delle tradizionali libertà costituzionali? Ovvero, è necessario ri-scrivere nuove norme costituzionali per definire le libertà che si sono venute a determinare a seguito dell'avvento della tecnologia, oppure si possono interpretare le vigenti norme costituzionali ricavandone da esse le nuove figure giuridiche dei nuovi diritti di libertà?» (T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. inf. e informatica*, 2020, p. 467).

[8] Il riferimento è, come noto, a O.S. KERR, *Digital Evidence and the New Criminal Procedure*, in *Columbia Law Review*, 2005, p. 279 ss., il quale auspicava, già anni or sono, l'adeguamento delle norme del codice di rito e dei principi a esso sottesi alle nuove metodologie di indagine informatica. In argomento, v. anche S. QUATTROCOLO, *Qualcosa di meglio del diritto (e del processo) penale?*, in F. Consulich – M. Miraglia – A. Peccioli (a cura di), *Alternative al processo penale? Tra deflazione, depenalizzazione,* diversion *e prevenzione*, Torino, 2020, p. 169 ss. e, spec., p. 170.

[9] L'espressione vuole ricomprendere l'impiego delle metodologie di indagine *on the social* in tutte le fasi che contraddistinguono il sistema penale (*intelligence*, prevenzione e repressione/accertamento).

[10] La proposta è stata avanzata da Lori Andrews, *Distinguished Professor* presso l'*Illinois Institute of Technology Chicago-Kent College of Law*, reperibile al sito *http://www.socialnetworkconstitution.com/the-social-network-constitution.html*. Lo stretto rapporto che intercorre tra il mondo *social* e i diritti fondamentali della persona è stato efficacemente messo in luce da S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 383, ove ricorda che la popolarità raggiunta da *Facebook* all'indomani della caduta dei regimi autoritari nordafricani

naviganti del *web*, nonché le relazioni interpersonali *ivi* coltivate, questa "Carta dei valori 2.0" si propone, da un lato, di trasfondere nel contesto virtuale diritti tradizionali, quali, ad esempio, la libertà di parola, di espressone e il diritto al controllo della propria immagine; e, dall'altro, di configurare inedite declinazioni di prerogative analogiche, quali un «*right to Due Process of Law in a social network context*» o forme di «*right to privacy in one's social networking profiles*». L'obiettivo che si intende perseguire è, in altre parole, quello di rintracciare nelle libertà fondamentali della persona un limite all'attività conoscitiva del rito nella fase preliminare.

Sennonché, la condivisibile e doverosa esigenza di rimodulare l'estensione delle libertà costituzionali e convenzionali non deve condurre verso forme di «garantismi inquinati»[11], tanto più in un'epoca storica nella quale al processo penale è richiesto di far fronte a una criminalità sempre più spietata, evoluta e tecnologicamente attrezzata, «pena la [sua] trasformazione in un'arma spuntata, inidonea a raggiungere lo scopo»[12]. Lo *ius investigandi*, da questo punto di vista, rappresenta l'antecedente logico-necessario per tutelare efficacemente la sicurezza dei *cives*; per dirla con le (condivisibili) parole della Corte costituzionale, «l'esigenza di acquisizione della prova del reato» costituisce un «valore primario sul quale si fonda ogni ordinamento»[13].

A tal proposito, in effetti, non può ragionevolmente dubitarsi del fatto che la sicurezza – secondo accreditate ricostruzioni dogmatiche[14] – rappresenti un valore "superprimario" che si pone quale substrato necessario di ogni collettività giuridica e, contestualmente, quale esigenza individuale e collettiva che incide sui bisogni della singola persona. Al contempo, però, deve parimenti riconoscersi come la necessità di garantire efficacemente la *tranquillitas* sociale possa inficiare negativamente su alcune libertà fondamentali. È questa, del resto, l'«intima contraddizione della procedura penale»[15]: le finalità cognitive, che spingono a dilatare i confini dell'indagine, sono chiamate a fare i conti con le prerogative riconosciute ai singoli individui. Il quesito al quale occorre rispondere, dunque, è sempre il medesimo, e tende a riproporsi, immutato, in ogni epoca: «il bene dell'amministrazione della

---

aveva indotto «molti attivisti a identificare questo successo con lo strumento che più visibilmente gli era stato associato, sì che si è chiesto che *Facebook* venisse riconosciuto come diritto fondamentale della persona».

[11] Si riprende l'espressione di A. GIARDA, *Persistendo 'l reo nella negativa*, Milano, 1980, p. 10.

[12] C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. proc.*, 2018, p. 1210. Come sottolineato anche da G. UBERTIS – V. PALTRINIERI, *Intercettazioni telefoniche e diritto umano alla privatezza*, in *Riv. it. dir. proc. pen.*, 1979, p. 603, «gli organi di polizia (sia di sicurezza che giudiziaria) e la magistratura devono essere dotati di mezzi adeguati e di uomini anche tecnologicamente preparati, in modo da raggiungere il massimo grado di efficienza possibile contro il terrorismo e la delinquenza».

[13] Corte cost., 27 giugno 1996, n. 238.

[14] G. CERRINA FERONI – G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi Costituzionali*, 2008, 1, p. 31. Nella medesima prospettiva, v., di recente, R. BIN, *Critica della teoria dei diritti*, cit., p. 13, il quale afferma perentoriamente che «la protezione della sicurezza dei cittadini è una prestazione fondamentale richiesta alle autorità pubbliche». Il dibattito, in particolare sul versante costituzionalistico, sulla definizione del concetto di sicurezza e sul suo fondamento nella Carta delle Leggi è ancora particolarmente vivace. Per una diversa e contrapposta visione rispetto a quella fatta propria dagli A. poc'anzi richiamati, cfr., per tutti, le imprescindibili riflessioni di A. BARATTA, *Diritto alla sicurezza o sicurezza dei diritti?*, in S. Anastasia – M. Palma (a cura di), *La bilancia e la misura*, Milano, 2001, p. 22 ss..

[15] A. CAMON, *Sfondi*, in AA.VV., *Fondamenti di procedura penale*, Milano, 2020, p. 7.

giustizia […] può essere prevalente al punto da subordinarvi beni ed interessi, come quelli della difesa, della libertà personale […], della riservatezza?»[16].

Sotto tale profilo, è doveroso ricordare, altresì, come il diritto alla sicurezza risulti intimamente connesso al principio di accertamento e di repressione dei reati che, sebbene non trovi espressa menzione all'interno della Carta fondamentale, appare senz'altro meritevole di tutela, alla luce del combinato disposto degli artt. 2 e 112 Cost[17]. Il perseguimento delle condotte illecite, difatti, non può che considerarsi la più evidente estrinsecazione del bisogno di sicurezza, a sua volta manifestazione di «un interesse pubblico primario, costituzionalmente rilevante, il cui soddisfacimento è assolutamente inderogabile»[18] e al quale devono concorrere tanto il diritto sostantivo, quanto il diritto processuale[19].

Da quanto detto, non può certo ricavarsi l'assunto secondo cui il processo penale dovrebbe essere concepito in termini repressivi, ovverosia come compartecipe all'obiettivo sanzionatorio, tipicamente affidato, in via esclusiva, al diritto sostantivo[20]: esso, è noto, ha finalità squisitamente cognitive, atte a tutelare, nel rispetto delle garanzie individuali fissate dal "diritto formale"[21], l'accertamento giurisdizionale del fatto di reato[22].

Se quanto osservato appare indubitabile, è appena il caso di notare, tuttavia, come il rito criminale, legandosi intimamente al "dovere di punire", costituisce l'unico strumento idoneo a consentire la realizzazione di quella funzione "incriminatrice" propria del diritto penale sostanziale; di talché, esso, com'è stato autorevolmente rilevato, concorre ad assolvere,

[16] Testualmente, benché in altro contesto, A. GIARDA, *Persistendo 'l reo nella negativa*, cit., p. 10. Per una rappresentazione del procedimento penale come luogo nel quale i «diritti individuali stanno in un rapporto di costante tensione con l'esigenza di garantire l'effettività dell'iniziativa processuale e, in definitiva, con l'esigenza repressiva», v. R. ORLANDI, *Garanzie individuali ed esigenze repressive (ragionando intorno al diritto di difesa nei procedimenti di criminalità organizzata)*, in AA.VV., *Studi in ricordo di Giandomenico Pisapia*, vol. II, Milano, 2000, p. 552.

[17] Il principio *de quo* appare senz'altro meritevole di tutela alla luce del combinato disposto delle suddette disposizioni costituzionali, volte a garantire l'interesse «a reprimere reati e a perseguire in giudizio coloro che delinquono» (così, Corte cost., 17 luglio 1998, n. 281). In tal senso, v., esplicitamente, anche C. CONTI, *Sicurezza e riservatezza*, in *Dir. pen. proc.*, 2019, p. 1572.

[18] Lapidariamente, ma in maniera assai incisiva, Corte cost., 23 luglio 1991, n. 366. Pure l'art. 159, comma 2, del d.lgs. 31 marzo 1998, n. 112, definisce l'«ordine pubblico e sicurezza pubblica» come «le misure preventive e repressive dirette al mantenimento dell'ordine pubblico, inteso come il complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale, nonché alla sicurezza delle istituzioni, dei cittadini e dei loro beni».

[19] Sul punto, v. D. PULITANÒ, *Sui rapporti tra diritto penale sostanziale e processo*, in *Riv. it. dir. proc. pen.*, 2005, p. 959.

[20] Come sottolinea O. MAZZA, *Le persone pericolose (in difesa della presunzione d'innocenza)*, in *Dir. pen. cont.*, 20 aprile 2012, p. 2, «interpretando rigorosamente il dettato costituzionale, nessuno può seriamente dubitare che il processo debba rimanere un giardino inviolato, deputato esclusivamente alla verifica della responsabilità per un fatto penalmente rilevante, senza essere gravato da fini impropri […] di repressione della devianza». Cfr., sul punto, anche F. CAPRIOLI, *Sicurezza dei cittadini e processo penale*, in M. Donini – M. Pavarini (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, p. 143, il quale ricorda, richiamando il pensiero del Pagano e del Romagnosi, come, invece, «l'idea che la sicurezza dei cittadini […] sia un bene destinato a ricevere tutela dal processo penale più ancora che dalla legge penale sostanziale è un'idea che vanta una tradizione illustre nella dottrina processualistica».

[21] *Rectius*, Costituzione e codice di procedura penale.

[22] In questi termini, G. SABATINI, *Principi di diritto processuale penale*, vol. I, Catania, 1948, p. 39 s.

sebbene in via meramente riflessa, un'indiretta finalità di difesa sociale-collettiva[23]. È per tale motivo, del resto, che il processo penale è stato icasticamente descritto come uno «strumento di produzione di risposte sanzionatorie»[24], locuzione con la quale si allude, per l'appunto, al fatto che l'accertamento, pur seguendo le regole e le forme stabilite del diritto processuale penale, è, in fondo, un «evento imposto dal diritto penale sostanziale»[25], l'unico in grado di legittimare l'irrogazione di una pena a seguito dell'accertamento di colpevolezza. Un rito penale, in altre parole, quale luogo di soddisfacimento di esigenze repressive attraverso il modello garantista del giusto processo[26]. Diversamente opinando, non sarebbe possibile – come sostenuto, invece, da autorevole dottrina – tutelare il processo «con mezzi che […] possono risolversi in più o meno intensi doveri di sopportazione imposti ai singoli e in più o meno drastiche compressioni di diritti individuali»[27].

Prendendo le mosse da tale inquadramento, si può osservare, tuttavia, come il dibattito sviluppatosi sul tema abbia spesso finito per esasperare, in maniera niente affatto condivisibile, una netta contrapposizione tra chi ritiene che la sicurezza collettiva rappresenti un valore tale da legittimare forme di «diritto penale del nemico»[28] e chi, per converso, tende a liquidare «ogni istanza relativa alla sicurezza […] come meramente "securitaria" o demagogica, e perciò solo non degna di seria attenzione»[29], senza tener conto, invece, che il bisogno di sicurezza (*rectius*, il principio di persecuzione penale) – a determinate condizioni – ben può giustificare la limitazione delle libertà individuali nel corso del procedimento, senza che ciò vada a detrimento della presunzione di non colpevolezza.

Entrambe le istanze, a ben considerare, meritano di essere prese sul serio[30], non foss'altro perché, in assenza della prima – come si è accennato – verrebbe meno la ragion d'essere dello stesso ordinamento statuale (di diritto) che, per sua natura, si fonda sulla necessità di

---

[23] Così si esprime, esplicitamente, V. GREVI, *Garanzie individuali ed esigenze di difesa sociale nel processo penale*, in L. Lanfranchi (a cura di), *Garanzie costituzionali e diritti fondamentali*, Roma, 1997, p. 261 s.

[24] F. VIGANÒ, *Terrorismo, guerra e sistema penale*, in *Riv. it. dir. proc. pen.*, 2006, p. 688, nt. 97.

[25] A.A. DALIA – M. FERRAIOLI, *Manuale di diritto processuale penale*, Padova, 2018, p. 25.

[26] In termini non dissimili si esprime D. PULITANÒ, *Sui rapporti tra diritto penale sostanziale e processo*, cit., p. 963.

[27] R. ORLANDI, *Garanzie individuali ed esigenze repressive*, cit., p. 555. Si tratta, a ben considerare, di una legittima esigenza che trova conforto nell'idea per cui il rito deve «saper produrre accertamenti di responsabilità; senza di che, girerebbe a vuoto, e ciò finirebbe per mettere in crisi la stessa tenuta delle garanzie liberali» (così, D. PULITANÒ, *Sui rapporti tra diritto penale sostanziale e processo*, cit., p. 970).

[28] È l'impostazione notoriamente sostenuta da G. JACOBS, *I terroristi non hanno diritti*, in R.E. Kostoris – R. Orlandi (a cura di), *Contrasto al terrorismo interno e internazionale*, Torino, 2006, p. 3 ss., il quale teorizza la distinzione tra un "diritto penale del nemico", applicabile a coloro che compiono azioni finalizzate a sovvertire l'ordinamento costituito e, per ciò stesso, paragonati a "non persone", e un "diritto penale del cittadino", dedicato a coloro che, pur violando le regole di pacifica convivenza, non contestano la legittimità del potere statale.

[29] Così, in una prospettiva condivisibilmente critica rispetto all'indirizzo esegetico (e, prima ancora, culturale) volto a sminuire l'importanza del valore della sicurezza nella società moderna, N. ZANON, *Un diritto fondamentale alla sicurezza?*, in *Dir. pen. proc.*, 2019, p. 1557.

[30] La necessità di individuare il "giusto mezzo" nella predisposizione della normativa processuale è stata recentemente messa in evidenza, in maniera cristallina, da M. GIALUZ – J. DELLA TORRE, *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022, p. 10, nt. 50, ove gli A. richiamano un passaggio di uno scritto di Alessandro Stoppato del 1912, nel quale l'autorevole giurista rileva come «la preponderanza dei mezzi inquisitori ed accusatori fece scattare una rivoluzione giuridica a difesa della libertà individuale, una rivoluzione giuridica in opposto farebbe sorgere la preponderanza dell'attività dell'imputato per esigenza di sicurezza».

garantire la civile convivenza tra cittadini[31] e, dunque, la sicurezza, presupposto necessario per il raggiungimento della "pace sociale".

Se è doveroso, pertanto, che il costituzionalismo del secondo dopoguerra si muova nel solco di quel "principio di massima espansione delle libertà individuali"[32] – dal quale si è ricavato un approccio diretto a privilegiare i diritti dell'imputato quale *focus* dell'attività legislativa e dommatica nel contesto del rito penale (sulla scorta del noto insegnamento di Francesco Cararra) – non può sottacersi, tuttavia, l'importanza da riconoscersi all'interesse (o al diritto?) della collettività al perseguimento dei crimini[33]. Quest'ultimo, a tutto concedere, non rappresenta affatto una «pulsion[e] antiliberal[e] a cui va opposta la tradizione gloriosa della difesa costituzionale dei diritti: altri diritti stanno dietro all'azione dei pubblici poteri, quelli atavici dalla cui tutela è iniziata la gloriosa storia dello Stato di diritto»[34].

Parimenti, però, va riconosciuto come la menomazione delle garanzie individuali rischi di determinare la più evidente contraddizione nella quale potrebbe incorrere un modello processuale accusatorio: in nome di quella legittima esigenza securitaria si finirebbe per calpestare quelle stesse libertà che si vorrebbero tutelare. È proprio questo, del resto, il «limite di carattere generale al proliferare delle tecniche investigative che attentano» ai diritti fondamentali: la «natura "democratica" della società»[35]. In definitiva: «la sicurezza non è il dio», ma i diritti, a loro volta, non sono «idoli intangibili»[36].

Se si accoglie, pertanto, l'idea che il processo penale è chiamato a svolgere esclusivamente una funzione di accertamento, il legislatore può legittimamente restringere i diritti del singolo che vi partecipa. Il *punctum dolens*, casomai, riguarda l'individuazione del limite all'esercizio di questo potere e, cioè, fino a dove l'ordinamento può dirsi legittimato, specialmente in sede di indagine, a realizzare attività intrusive nella sfera inviolabile della persona. Detto altrimenti: se la procedura penale non è un «luogo deputato ad esercitare

---

[31] C. BECCARIA, *Dei delitti e delle pene*, (1764), Parigi, 1828, p. 6 ss. È questa, del resto, la visione statuale rappresentata dal pensiero di Hobbes che, lungi dall'incarnare «il teorico dell'assolutismo per antonomasia», rappresenta «il precursore dello Stato di diritto». D'altro canto, «la sicurezza dei cittadini e la loro eguaglianza di fronte alla legge» sono capisaldi dell'intera costruzione teorica dell'illustre filosofo. Per questa ri-lettura della tradizionale visione del pensiero hobbesiano, v., anche per ulteriori riferimenti bibliografici a sostegno, le riflessioni di R. BIN, *Critica della teoria dei diritti*, cit., p. 11 ss.

[32] Scontato, ma doveroso, il rinvio a P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, p. 41, il quale, nel celebre passaggio, si esprime come segue: «una regola, inespressa nel diritto positivo, ma totalmente pacifica in letteratura, tanto da essere data quale presupposto costante dell'interpretazione, è quella della presunzione della massima espansione delle libertà costituzionali; che significa interpretazione estensiva delle norme relative, tendente ad affermare la massima ampiezza da riconoscere alla libera sfera di attività dell'individuo e del gruppo».

[33] Cfr., in proposito, le pungenti considerazioni di F. VIGANÒ, *Terrorismo, guerra e sistema penale*, cit., p. 688: «a me pare che la scienza penalistica italiana dovrebbe porsi il problema se negli ultimi decenni non abbia pensato un po' troppo al diritto penale come *magna charta* del reo – come strumento, cioè, di garanzia dei diritti fondamentali dell'imputato e del condannato –, piuttosto che come strumento che, al tempo stesso, è chiamato ad assicurare una efficace difesa dei beni giuridici individuali e collettivi minacciati dalla criminalità».

[34] R. BIN, *Critica della teoria dei diritti*, cit., p. 67.

[35] F. CAPRIOLI, *Sicurezza dei cittadini e processo penale*, cit., p. 147 s.

[36] Si esprime in questi termini, F. VIGANÒ, *Terrorismo, guerra e sistema penale*, cit., p. 690.

potere», quanto, piuttosto, un insieme di «regol[e] destinat[e] a limitalo»[37], occorre chiedersi se e come tale limitazione possa realizzarsi.

La risposta al quesito non può che essere rintracciata nella Carta delle Leggi: quale "tavola di valori" che esprime il comune sentire di una società in un determinato momento storico, la Costituzione (e le fonti europee sovraordinate) è l'unica fonte alla quale occorre rivolgersi per individuare tanto i singoli diritti fondamentali di volta in volta in rilievo, quanto l'*an* e il *quomodo* di eventuali restrizioni[38]. Se in uno Stato di diritto (perlomeno quello di derivazione liberale-continentale) la regola è la libertà, qualunque restrizione a essa imposta, pur giustificata dalla legittima istanza di accertamento dei reati, deve essere esplicitamente ammessa dalla Fonte suprema ed espressamente disciplinata da una norma giuridica[39], in ossequio al noto principio secondo cui «ogni atto processuale ha presupposti di legittimità indicati dalla legge»[40].

È questo, a ben riflettere, il nodo centrale dei rapporti tra le nuove metodologie di "indagine 2.0" e i diritti fondamentali dell'indagato (e dei terzi interessati dalle misure): se, a fronte di una iper-specializzazione della delinquenza, l'inchiesta penale non può oggi rinunciare all'impiego di tecniche investigative a contenuto tecnologico[41], l'unica via per legittimare siffatte intrusioni è l'individuazione di una regolamentazione che giustifichi la limitazione della libertà entro gli stretti confini di quanto consentito dal dettato costituzionale e dai

[37] M. NOBILI, *Scenari e trasformazioni del processo penale*, Padova, 1998, p. 190.

[38] Per riprendere le parole di P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., p. 41, i diritti «nascono come li raffigura il diritto positivo, coi soli limiti che la stessa costituzione eventualmente pone nel mentre li raffigura (cioè nel contesto delle norme istitutive)». Altrettanto incisive, sul punto, le parole di G. AMATO, *Individuo e autorità nella disciplina della libertà personale*, Milano, 1967, p. 309, per il quale «la disciplina costituzionale si caratterizza […] per un dato costante, per la puntuale identificazione, cioè, degli interessi ai quali ciascuna libertà può essere subordinata dalla legge, ovvero dei modi nei quali il limite può essere imposto». Ed è per questo che, in nessun caso, le norme costituzionali «possono essere ritenute di intralcio all'apparato di coercizione; del quale, piuttosto, costituiscono (o debbono costituire) una condizione di funzionalità» (G. RICCIO, *Politica penale dell'emergenza e Costituzione*, Napoli, 1982, p. 101).

[39] Come hanno ricordato a più riprese i giudici costituzionali, del resto, «ogni limitazione di diritti fondamentali deve partire dall'assunto che, in presenza di un diritto inviolabile, il suo contenuto di valore non può subire restrizioni o limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante» (Corte cost., 11 luglio 1991, n. 366; Corte cost., 5 luglio 2010, n. 249).

[40] È questa la definizione di legalità processuale offerta da P. NUVOLONE, *Legalità penale, legalità processuale e recenti riforme*, in *Riv. it. dir. proc. pen.*, 1984, p. 3.

[41] Di questa stessa opinione, con riguardo ai nuovi "mezzi di ricerca della prova 2.0", è anche W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Milano, 2021, p. 261. Del resto, già illustre dottrina, agli albori degli anni '80, sottolineava la necessità di «modernizzare e specializzare» gli organi di polizia, dal momento che questi «non devono continuare ad operare isolati, con strumenti arcaici, in una torre d'avorio, ma devono essere muniti di una preparazione che permetta loro di conoscere [e affrontare] l'individuo delinquente» (P. NUVOLONE, *Funzionamento e prospettive della giustizia penale in un mondo in evoluzione*, in *Ind. pen.*, 1983, p. 240).

principi da esso ricavabili (proporzionalità, adeguatezza, etc.)[42]. Si ravvisa, in tal modo, «una vera e propria "legittima difesa" dello Stato di fronte all'inasprirsi della criminalità»[43].

È solo in questa prospettiva, allora, che si può tentare di offrire una risposta al quesito posto *in apicibus*.

In un'epoca storica nella quale le strumentazioni tecnologiche stanno modificando il modo di vivere e di relazionarsi con il prossimo, l'unica via che appare perseguibile è quella di valutare caso per caso se le libertà tradizionali sono ancora capaci di garantire il cittadino dalle intrusioni informatiche, tenendo ben presente che, da un lato, nessun diritto può essere considerato assoluto o «tiranno»[44], giacché ogni libertà vive in un sistema complesso in cui i diritti, compresi quelli costituzionalmente garantiti, devono essere bilanciati con principi concorrenti. E, dall'altro, non deve mai dimenticarsi, però, che «l'accusa [penale] può colpire qualsiasi cittadino, sicché l'autorità sociale deve moderare l'uso degli strumenti processuali muovendo dal presupposto che gli stessi sempre incombono su un possibile innocente»[45]. Il potere investigativo, come si è detto, dovrebbe sempre rappresentare un'eccezione alla regola di libertà.

2. Le libertà "di relazione" nel *web* 2.0: segretezza, riservatezza e intimità della vita privata

Segretezza delle comunicazioni, riservatezza dei propri dati e intimità delle attività svolte nel contesto privato rappresentano tre categorie giuridiche che, pur con le proprie peculiarità[46], esprimono, nell'attuale contesto sociale, una matrice unitaria: assicurare la tutela dell'"Io informatico"[47] a fronte di possibili e illegittime ingerenze del potere pubblico nella sfera di libertà individuale.

Sembra essersi delineato, in questa prospettiva, un vero e proprio diritto generale e astratto «dell'individuo a sottrarsi al controllo della società»[48]. In un mondo nel quale la persona si identifica con i propri dati[49] e le informazioni circolano in un etere impalpabile, si è fatta via via sempre più pressante l'esigenza di garantire questo "trinomio di libertà" che, come si

[42] Questo concetto è stato espresso, in maniera alquanto efficace, nella recente sentenza con la quale la Corte costituzionale ha dichiara l'illegittimità dell'art. 3, comma 4, del d.lgs. 6 settembre 2011, n. 159, nella parte in cui include i telefoni cellulari tra gli apparati di comunicazione radiotrasmittente di cui il questore può vietare, in tutto o in parte, il possesso o l'utilizzo: «le esigenze di prevenzione e difesa sociale ben possono giustificare, si è detto, misure restrittive, e queste possono incidere anche su diritti fondamentali. Ma, proprio ove ciò accada, le garanzie costituzionali reclamano osservanza» (Corte cost., 12 gennaio 2023, n. 3).

[43] P. TONINI – C. CONTI, *Il diritto delle prove penali*, Milano, 2014, p. 483.

[44] Il riferimento, com'è noto, va all'icastica espressione utilizzata dai giudici costituzionali in occasione di una delle pronunce sul cd. caso Ilva (Corte cost., 9 maggio 2013, n. 85).

[45] R. ORLANDI, *Rito penale e salvaguardia dei galantuomini*, in *Criminalia*, 2006, p. 297.

[46] Secondo l'opinione prevalente in dottrina, mentre la segretezza è volta a impedire che soggetti diversi dal destinatario prendano parte ad una comunicazione, la riservatezza consiste nell'aspirazione dei colloquianti che una determinata notizia non fuoriesca dal loro patrimonio conoscitivo (G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Milano, 1983, p. 3; L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, p. 12 ss.).

[47] Di «corpo elettronico» parla S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014, p. 44.

[48] G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, cit., p. 2.

[49] Cfr., ancora, S. RODOTÀ, *Il mondo nella rete*, cit., p. 44, per il quale «noi siamo i nostri dati».

avrà modo di osservare, assume oggi una certa consistenza tanto sotto il profilo individuale, quanto collettivo-relazionale.

3. Nuove forme di comunicazione e interpretazioni evolutive dell'art. 15 Cost.: *Whatsapp*, *Telegram* e le altre piattaforme di messaggistica istantanea

Muovendo dalla garanzia contenuta all'art. 15 Cost., la Corte costituzionale ha da tempo sottolineato come «l'inderogabile dovere di prevenire e reprimere i reati deve essere svolto nel più assoluto rispetto di particolari cautele dirette a tutelare un bene, l'inviolabilità della segretezza e della libertà delle comunicazioni, strettamente connesso alla protezione del nucleo essenziale della dignità umana»[50]. Emerge, in questa visione, lo stretto legame che intercorre tra il diritto di comunicare liberamente e il pieno sviluppo della personalità individuale, sia come singolo, sia nelle formazioni sociali (art. 2 Cost.).

Non è necessario, ai fini dell'analisi che si va conducendo, esaminare, *funditus*, il significato e l'estensione delle tutele di cui all'art. 15 Cost.[51]. Ciò nondimeno, va preso atto che la disposizione costituzionale garantisce sia la libertà di comunicare con altri soggetti senza alcuna limitazione oggettiva o soggettiva, nonché senza alcuna interferenza da parte di privati o di pubblici poteri, sia la segretezza della comunicazione in senso stretto, cioè, la pretesa che terzi estranei al colloquio non ne apprendano illegittimamente il contenuto[52]. Proprio al fine di evitare indebite compressioni da parte del potere pubblico, i Padri Fondatori hanno previsto che ogni sua limitazione possa avvenire soltanto per atto motivato dell'autorità giudiziaria (riserva di giurisdizione[53]) con le garanzie previste dalla legge (riserva di legge).

È, però, in relazione al contenuto del precetto che si pongono non pochi problemi di carattere interpretativo, con specifico riguardo proprio al tema oggetto della presente trattazione.

Preso atto che la Costituzione non fornisce una definizione chiara e precisa del concetto di "comunicazione" (e, invero, neppure di "corrispondenza"), la dottrina, specie quella costituzionalista, ne ha offerto una nozione particolarmente estesa[54], ricomprendendovi qualunque trasmissione di pensieri tra due o più soggetti determinati «col mezzo di cose atte a fissare […] o ricevere l'espressione del pensiero»[55]. Si è osservato, altresì, come appaia

[50] Corte cost., 26 febbraio 1993, n. 81.

[51] Cfr., per tutti, P. BARILE – E. CHELI, voce *Corrispondenza (libertà di)*, cit., p. 743 ss.

[52] V. ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni*, Torino, 1963, p. 91.

[53] Sul dibattito in merito alla nozione di «autorità giudiziaria» di cui all'art. 15 Cost. e alla possibilità di ricomprendervi o meno anche l'organo d'accusa, v., per la tesi positiva, A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, p. 109 s., e, per quella negativa, L. FILIPPI, *L'intercettazione di comunicazioni*, cit., p. 61 s.

[54] Di un «concetto valvola» ha parlato A. VALASTRO, *Libertà di comunicazione e nuove tecnologie. Inquadramento costituzionale e prospettive di tutela delle nuove forme di comunicazione interpersonale*, Milano, 2001, p. 118.

[55] P. BARILE – A. CHELI, voce *Corrispondenza (libertà di)*, cit., p. 744. Per una nozione particolarmente estesa di comunicazione, v., più di recente, sul versante processuale, E.M. MANCUSO, *L'acquisizione di contenuti* e-mail, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 514, il quale si riferisce a una «trasmissione di dati, di contenuti idonei a rappresentare un messaggio o, ancora, un qualsiasi elemento raffigurativo (immagine, contenuto audio, contenuto video) che permetta di arricchire il patrimonio cognitivo

del tutto irrilevante il tipo di mezzo cui il mittente si serve per riversare all'esterno il contenuto comunicativo[56].

Quest'ultima considerazione merita di essere approfondita.

È pur vero che l'impiego di uno strumento piuttosto che un altro può astrattamente incidere sul grado di segretezza della comunicazione. Tuttavia, ciò che rileva, ai fini del suo inquadramento all'interno della fattispecie di cui all'art. 15 Cost., è la portata unidirezionale, personale e segreta dello scambio informativo, ossia il fatto che esso sia diretto a uno o più soggetti determinati; elemento, quest'ultimo, che consente di distinguere la libertà di comunicazione dalla libertà di informazione e manifestazione del pensiero (art. 21 Cost.). È la dottrina costituzionalista, ancora una volta, a tracciare la via: si ha corrispondenza *lato sensu* intesa quando i destinatari del messaggio sono predeterminati e la comunicazione tende alla segretezza; per contro, si ha manifestazione del pensiero quando la sua diffusione è diretta a un pubblico indistinto[57]. Per di più, giova osservare, a sostegno di tale esegesi, come la Costituzione non ponga alcun limite di carattere formale e letterale al *modus comunicandi*, dovendosi ritenere protetto ogni scambio di idee, purché realizzato con un mezzo che attribuisca alla comunicazione il crisma della segretezza.

Quanto osservato acquista particolare importanza sul versante della trasmissione di dati nell'ambito dei *social network*.

Le piattaforme di *sharing*, come acutamente osservato, non mettono in discussione le tradizionali categorie concettuali (si legga, quelle di cui agli artt. 15 e 21 Cost.), bensì «determinano l'esistenza di una zona grigia» nella quale si collocano «forme "ibride" di comunicazione telematica»[58]. La circostanza che i cibernauti possano usufruire, alternativamente e contemporaneamente, di servizi di comunicazione e di servizi di condivisione rende arduo – o, secondo taluno, financo impossibile[59] – individuare il paradigma costituzionale di riferimento e, di conseguenza, le tutele azionabili a fronte di un'invasione nella sfera privata dell'individuo. Nell'universo *social*, in effetti, non è sempre agevole ricondurre la singola esternazione di un pensiero nell'ambito di una vera e propria comunicazione – cui segue l'applicazione delle garanzie previste all'art. 15 Cost – ovvero nell'ambito di una più generale condotta diffusiva o divulgativa realizzata nella propria "sfera sociale", rivolta, perciò, a destinatari non predeterminati (art. 21 Cost.)[60]. Le

---

del destinatario». Per un'interpretazione più restrittiva, v., invece, A. PACE, *Problematica delle libertà costituzionali. Lezioni (Parte speciale – I)*, Padova, 1985, p. 242.

[56] P. BARILE – A. CHELI, voce *Corrispondenza (libertà di)*, cit., p. 744.

[57] Su questa distinzione, v., per tutti, P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., p. 163.

[58] A. PAPA, *Espressione e diffusione del pensiero in* Internet. *Tutela dei diritti e progresso tecnologico*, Torino, 2009, p. 109. Pure S. SIGNORATO, *Le indagini digitali*, cit., p. 70, sottolinea come in Rete tendano a sfumare «le distinzioni che connotano le diverse libertà tradizionali, dato che proprio in rete, in una sorta di sincrasi delle varie libertà, nello stesso tempo o in tempi assai ravvicinati, ci si esprime, ci si riunisce, si corrisponde, ecc.».

[59] M. OROFINO, *L'articolo 15 della Costituzione italiana: osservazioni sulla libertà e sulla segretezza delle comunicazioni ai tempi del* web *2.0*, in T.E. Frosini – O. Pollicino – E. Papa – M. Bassini (a cura di), *Diritti e libertà in* Internet, Milano, 2017, p. 205.

[60] Su questa difficoltà, v., più approfonditamente, M. OROFINO, *L'articolo 15 della Costituzione italiana*, cit., p. 193 ss. e, spec., p. 194, ove si sottolinea che i *social network* «rendono, infatti, la linea di demarcazione tra comunicazione, diffusione e persino altre attività in cui la comunicazione è solo strumentale assai opaca sia perché i nuovi servizi in sé si prestano a svariati utilizzi nonché a cambiare d'uso in corso d'opera sia perché è

trasmissioni di pensiero, realizzate attraverso un profilo *social* che gode di centinaia o migliaia di *followers*, ad esempio, possono essere comunque considerate alla stregua di comunicazioni riservate in quanto dirette a una platea predefinita di soggetti (*rectius*, "i seguaci")[61]?

Indubbiamente più agevole è, per contro, l'attività esegetica volta a ricondurre nella copertura offerta dall'art. 15 Cost. le comunicazioni effettuate attraverso le applicazioni di messaggistica istantanea messe a disposizione dai gestori dei principali *social network* (*Whatsapp*, *Facebook Messanger*, *Telegram*, etc.).

Sotto un primo profilo, come si è osservato, se la forma adoperata è ininfluente per individuare il campo di applicazione dell'art. 15 Cost., anche queste nuove modalità di comunicazione debbono essere tendenzialmente ricondotte nell'orbita della disposizione costituzionale. In aggiunta, non sembra potersi dubitare della segretezza che caratterizza questo specifico scambio informativo realizzatosi *online*. L'impiego della crittografia, come si vedrà a breve, conferisce a queste interazioni digitali il carattere della confidenzialità, giacché il contenuto del messaggio può essere "visibile" solo al destinatario.

Diversamente opinando, la norma *de qua* si rivelerebbe inadeguata a far fronte alle sfide della società contemporanea; una società nella quale – è difficile non riconoscerlo – il concetto di «altre forme di comunicazione» di cui all'art. 15 Cost. include, perlopiù – ancorché non in via esclusiva –, strumenti di interazione 2.0, quali, appunto, i servizi di messaggistica istantanea come *Whatsapp* o *Telegram*. È la stessa *ratio* della disposizione costituzionale a imporre tali conclusioni: la formulazione volutamente elastica dell'art. 15 Cost. mira a «consentire alla norma di adattarsi agli sviluppi della tecnica e di riuscire a comprendere nuove possibili forme espressive, inimmaginabili all'epoca della redazione del testo»[62].

Una volta ricondotte le comunicazioni scambiate mediante le piattaforme di *instant messaging* sotto la copertura dell'art. 15 Cost. (e dell'art. 8 CEDU[63]), lo studioso è comunque chiamato a confrontarsi con problematiche di non poco momento, specie in relazione alle diverse modalità acquisitive cui è astrattamente possibile ricorrere per

---

la volontà dell'utente a essere sempre più spesso difficile da decifrare». In termini non dissimili, v. A. PAPA, *Espressione e diffusione del pensiero in* Internet, cit., p. 112. Nel panorama internazionale, per le medesime considerazioni, v. A. NIETO MARTÍN – M. MAROTO, *Redes sociales en internet y "data mining" en la prospección e investigación de comportamientos delictivos*, in *Revista de derecho penal y criminologia*, 2013, p. 41, p. 47. Tali problematiche erano già state colte, benché in un periodo antecedente alla diffusione dei *social network* e, in particolare, con riguardo ai messaggi affissi nei *newsgroup*, da A. VALASTRO, *Libertà di comunicazione e nuove tecnologie*, cit., p. 219.

[61] A tale interrogativo, pur con riguardo alle prime forme di videoconferenza via *Internet* o alle *Relay Chat*, si offriva una risposta negativa: «quando la cerchia dei soggetti con i quali il mittente intende comunicare si ampia oltre una certa misura è discutibile che possa ancora parlarsi di comunicazione riservata» (così, A. VALASTRO, *Libertà di comunicazione e nuove tecnologie*, cit., p. 145, per la quale il "bandolo della matassa" potrebbe essere sciolto riferendosi solamente alle «diverse modalità comunicative in concreto adottate e, più esattamente, all'attitudine di queste a comunicare messaggi a singoli o alla generalità»).

[62] P. GIOCOLI NACCI, *Libertà di corrispondenza*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, vol. XII, Padova, 1990, p. 121. Più di recente, v. Corte cost., 12 gennaio 2023, n. 3, cit., ove si sottolinea come la tutela della libertà (e della segretezza) della corrispondenza si estenda «ad ogni forma di comunicazione, aprendo così il testo costituzionale alla possibile emersione di nuovi mezzi e forme della comunicazione riservata».

[63] Esplicitamente, in tal senso, Corte edu, *Bărbulescu c. Romania*, 5 settembre 2017, par. 74.

incanalare le predette informazioni sui binari del procedimento penale. Come si avrà modo di osservare[64], l'alternativa che si presenta è pressoché riconducibile alla triade "documento, sequestro, intercettazione". A tal proposito, la tendenza della giurisprudenza italiana (e non solo), lo si vedrà più in dettaglio, è quella di ampliare oltremisura il ricorso al "contenitore probatorio" rappresentato dall'art. 234 c.p.p., finendo così per svilire la tutela (riserva di legge e riserva di giurisdizione) apprestata dall'art. 15 Cost.

4. Il cd. *data sharing* e il "naufragio" della *privacy* nei *social network*

Appaiono maggiormente complesse, per un duplice ordine di ragioni, le riflessioni che occorre svolgere con riguardo al diritto alla riservatezza.

Innanzitutto, non è affatto agevole individuare una nozione unitaria di tale concetto, trattandosi, com'è stato autorevolmente osservato, di un *quid* impalpabile e «variabile in funzione dei soggetti, dei momenti storici, dei luoghi»[65]. Del resto, la cosa più sorprendente del diritto *de quo* è che «tutti ne parlano, ma nessuno sembra avere un'idea chiara di che cosa sia»[66]. Si considerino, già a livello lessicale, i termini "*privacy*", "riservatezza", "privatezza"[67], "vita privata", "intimità della vita privata" sovente impiegati come sinonimi, ma, in realtà, rappresentativi di concetti non del tutto assimilabili[68].

A rendere ancor più difficoltosa l'opera esegetica, peraltro, concorre, sul versante nazionale, la mancata previsione, a livello costituzionale, di una qualche forma esplicita di tutela della *privacy* che, a ben considerare, ha ritardato e condizionato gli interventi legislativi in materia volti a garantirne un più ampio spettro applicativo.

L'omesso riferimento alla garanzia di riservatezza, come noto, ha generato una vivace disputa dottrinale circa la possibilità di ricondurla, in ogni caso, a una delle prerogative fondamentali già incardinate nella Carta. La tesi che sembra prevalere, in un dibattito tutt'ora ricco e variegato, è quella di un riconoscimento indiretto alla luce del combinato disposto degli artt. 2 Cost. e 8 CEDU[69].

---

[64] Cfr., spec., Parte II, Cap. V, par. 6.

[65] S. RODOTÀ, *La* privacy *tra individuo e collettività*, in *Pol. dir.*, 1974, p. 551. Ed è per questo motivo che autorevole dottrina ha fatto riferimento al concetto di *privacy* come a una «costellazione di diritti» (F. MODUGNO, *I «nuovi diritti» nella Giurisprudenza Costituzionale*, Torino, 1995, p. 20).

[66] J.J. THOMPSON, *The Right to Privacy*, in *Philosophy and Public Affairs*, 1975, p. 295 (trad. nostra).

[67] Ritenevano preferibile l'impiego di tale formula, sul finire degli anni '70 dello scorso secolo, G. UBERTIS – V. PALTRINIERI, *Intercettazioni telefoniche e diritto umano alla privatezza*, cit., p. 606, i quali si riferivano a quel «diritto […] a vedere "rispettato" e […] ad escludere dall'altrui conoscenza quanto a riferimento alla propria "intimità della vita privata"».

[68] P. PATRONO, voce Privacy *e vita privata* (dir. pen.), in *Enc. dir.*, vol. XXXV, Milano, 1986, p. 559.

[69] G. SILVESTRI, *L'individuazione dei diritti della persona*, in *Dir. pen. cont.*, 29 ottobre 2018, p. 8. Nello stesso senso, tra i processualisti, v., *ex plurimis*, E. ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della privacy e onde eversive*, in *Arch. pen.*, 2015, p. 918 s.; A. GAITO – S. FÙRFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen.*, 2016, p. 317 ss., i quali richiamano una risalente pronuncia della Corte costituzione che ha collocato il diritto alla riservatezza tra i diritti inviolabili «garantiti all'art. 2 Cost., in quanto in tale norma ricompresi gli artt. 12 della Dichiarazione Universale dei diritti dell'uomo e 8 della C.e.d.u.» (Corte cost., 5 aprile 1973, n. 38. Più di recente, cfr. Corte cost., 22 aprile 2009, n. 173); F. IOVENE, *Le c.d. perquisizioni on line tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont. – Riv. Trim.*, 2014, 3-4, p. 336.

Da un lato, la clausola generale e aperta contenuta nella disposizione costituzionale[70] consente di ricomprendere la riservatezza tra quei «diritti inviolabili dell'uomo» riconosciuti e garantiti dalla Repubblica.

Dall'altro, la norma pattizia – che deve ritenersi ormai parte integrante del sistema statale interno, in quanto norma interposta di rango costituzionale[71] – autorizza a incrementare un livello di tutela che, altrimenti, sarebbe decisamente scarno. Difatti, l'art. 2 Cost., contrariamente a quanto previsto agli artt. 13 ss. Cost., non contiene alcun riferimento né a una riserva di legge, né, tantomeno, a una riserva di giurisdizione. Per converso, l'art. 8 CEDU è stato oggetto da parte della Corte di Strasburgo di un'esegesi particolarmente estensiva per quanto concerne i confini applicativi (stabilendone l'operatività con riguardo a qualunque intromissione nella vita privata dei cittadini[72]) e condivisibilmente restrittiva in merito alle possibili interferenze statali con il diritto *ivi* tutelato. Necessarietà di una previsione legislativa (*i*), soddisfacimento di una tra le esigenze indicate dalla stessa disposizione (*ii*) e proporzionalità dell'intrusione (*iii*) sono i tre parametri enucleati dai giudici europei che rendono legittima l'attività penale investigativa volta alla prevenzione e alla repressione dei reati[73].

Non può essere sottaciuto, in una diversa prospettiva, come ogni attività di investigazione digitale, palese od occulta, sia ormai sempre potenzialmente in grado di ledere la riservatezza delle persone[74]. È proprio per tale motivo, d'altronde, che la *privacy* va assumendo un ruolo sempre più significativo nel contesto delle garanzie costituzionali e convenzionali atte a limitare l'esercizio dello *ius investigandi* di matrice pubblica.

Sebbene esuli dai confini della presente trattazione una disamina storico-giuridica dell'evoluzione dogmatica che ha interessato il diritto alla riservatezza[75], è comunque opportuno segnalare come la *privacy*, lungi dal dover essere interpretata come un mero «*right to be let alone*»[76], abbia oggi assunto i caratteri di un diritto fluido e malleabile, perfettamente confacente con quella «modernità liquida»[77] che contraddistingue l'attuale periodo storico.

Muovendo da una dimensione essenzialmente negativa e spiccatamente individualistica diretta a escludere terzi dalla propria sfera privata ("diritto di essere lasciati soli"), si è giunti

[70] A favore della natura "aperta", v., per tutti, A. BARBERA, sub *Art. 2*, in G. Branca (a cura di), *Commentario della Costituzione. Principi fondamentali*, Bologna, 1975, p. 65 ss.; F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen.*, 1967, p. 1094. *Contra* P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., p. 53 ss. Sull'essenziale «inutilità o scarsa utilità della questione», v., invece, F. MODUGNO, *I «nuovi diritti» nella Giurisprudenza Costituzionale*, cit., p. 2 ss.

[71] Il riferimento è alle note sentenze della Corte costituzionale n. 348 e 349 del 2009.

[72] Cfr. Corte edu, 12 maggio 2000, *Khan c. Regno Unito*.

[73] Cfr. Corte edu, 26 aprile 1979, *Sunday Times c Regno Unito*.

[74] Lo osservava, già, F. RUGGIERI, *Profili processuali nelle investigazioni informatiche*, in L. Picotti (a cura di), *Il diritto penale dell'informatica nell'epoca di* Internet, Padova, 2004, p. 154 ss.

[75] La letteratura sul punto, tanto monografica, quanto in rivista, è divenuta "tsunamica". Punto di riferimento restano, senza dubbio, le numerose opere di Stefano Rodotà (cfr. *supra* e *infra*).

[76] Secondo la nota definizione offerta dai "padri" della *privacy*, S.D. WARREN – L.D. BRANDEIS, *The Right to Privacy*, in *Harward Law Review*, 1890, 4, p. 193.

[77] Z. BAUMAN, *Vita liquida*, Bari, 2006.

ad affermare l'esistenza di un vero e proprio *habeas data*[78], espressione di un generale diritto al monitoraggio e al controllo sui propri dati personali. Quest'ultima esigenza, come noto, si è fatta sempre più incalzante in una società nella quale la raccolta e l'elaborazione massiva di informazioni costituiscono ormai la prassi in ogni attività umana connotata dall'impiego di strumenti tecnologici[79]. Il crescente ricorso a tecniche informatizzate che consentono di produrre un'immensa quantità di informazioni, d'altro canto, non poteva non riflettersi sulla nascita di un corrispondente diritto del singolo cittadino a «governare i dati che intimamente lo riguardano»[80].

Le nuove frontiere della *privacy* e della riservatezza, dunque, inducono a prospettare l'esistenza di un diritto alla tutela *lato sensu* intesa dei propri dati e, contestualmente, della propria intimità personale. Partendo dall'assunto secondo cui «esiste una costante relazione tra mutamenti delle tecnologie delle informazioni e mutamenti del concetto di *privacy*»[81], non stupisce che la riservatezza abbia conosciuto il suo periodo aureo e di massimo splendore (tanto in sede universitaria, quanto legislativa[82]) proprio con la diffusione di *Internet* su larga scala.

Sennonché, l'avvento dei *social network* pare aver generato una brusca e preoccupante inversione di tendenza alla quale il processualista deve guardare con vivo interesse.

E si spiega.

«*I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*»[83]. È questo il titolo di una fortunata opera pubblicata nel 2013 con la quale la accreditata dottrina ha messo in evidenza una delle principali conseguenze derivanti dall'impiego di massa delle piattaforme digitali di comunicazione: la "morte della *privacy*". Lo stesso ideatore di *Facebook*, Mark Zuckemberg, in un'intervista rilasciata al *New York Times* nel 2010, ha espressamente dichiarato che a seguito dell'avvento dei *social media* «*the age of privacy is over*»[84].

Benché la dottrina più autorevole[85] abbia messo in guardia, già agli inizi degli anni '70, dall'adottare approcci apocalittici in tema di *privacy* – all'epoca "assalita" dalla diffusione degli elaboratori elettronici –, le preoccupazioni manifestate oltreoceano sembrano cogliere nel segno.

È opinione comune, in effetti, che le "pagine *web* interattive" abbiano provocato una battuta d'arresto al processo di crescita e perfezionamento della "riservatezza 2.0" posto che, nell'attuale realtà cibernetica, nessuno può dirsi davvero al riparo da occhi indiscreti. Una

---

[78] Per un'ampia trattazione del tema, anche in una prospettiva europea, v., per tutti, C.E. PÉREZ-LUÑO ROBLEDO, *El procedimiento de Habeas Data. El derecho procesal ante las nuevas tecnologías*, Madrid, 2017.

[79] S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 397 s.

[80] Efficacemente, L. LUPÁRIA, Privacy, *diritto della persona e processo penale*, in *Riv. dir. proc.*, 2019, p. 1464.

[81] S. RODOTÀ, *La privacy tra individuo e collettività*, cit., p. 551.

[82] Si pensi all'approvazione nel 2003 del Codice *privacy* (d.lgs. 30 giugno 2003, n. 196).

[83] L. ANDREWS, *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*, Londra, 2013.

[84] *https://archive.nytimes.com/www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html?source=post_page*.

[85] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, 1973 (Ristampa anastatica a cura di G. Alpa), Napoli, 2018, p. 37.

delle caratteristiche principali delle piattaforme di *sharing*, come si è detto[86], è proprio quella di indurre i propri utenti (con l'impiego di tecniche di *design technology* ai limiti della coartazione psichica) alla condivisione di dati e informazioni, ancorché di carattere non necessariamente personale. La filosofia della condivisione – in contrapposizione alla valenza individuale della *privacy* – emerge anche dal linguaggio utilizzato all'interno dei *social network*: si parla, infatti, di visualizzazioni, condivisioni, visibilità, etc., tutte espressioni che mettono in risalto l'aspetto pubblico-relazionale dell'uomo a discapito di una dimensione squisitamente individuale-personale[87]. Nei *social network*, dunque, ciascuno alimenta l'aspetto pubblico della propria identità per dare senso (e risalto) all'aspetto privato, «si esibisce un insieme di informazioni personali, il corpo elettronico, così come si esibisce il corpo fisico attraverso tatuaggi, piercing e altri segni d'identità»[88].

Evidente è l'approdo del discorso: nella realtà *social* non è possibile vantare alcuna aspettativa di riservatezza.

A fronte di tale assioma, si sono andate sviluppando, sul versante processuale, due impostazioni metodologiche opposte, rispetto alle quali è lecito esprimere più di qualche perplessità.

Si assiste, da un lato, alla tendenza generalizzata, specialmente nel campo delle indagini a contenuto tecnologico, a voler superare la tradizionale distinzione tra segretezza e riservatezza, tra sfera privata e sfera pubblica[89], sul presupposto dell'esistenza di un unico spazio virtuale nel quale gli individui manifestano la propria personalità e realizzano le proprie attività *online*. Questa impostazione metodologica[90], ancorché mossa dal nobile (e condivisibile) intento di approntare una maggior tutela alle libertà fondamentali a fronte di tecniche di indagine sempre più invasive, rischia, però, di rivelarsi controproducente. Pur nella piena consapevolezza circa l'esistenza di "macrofagi investigativi" (si legga, ad esempio, il *trojan horse*) che si nutrono di qualsivoglia *bit* digitale – rispetto ai quali, in effetti, può essere ragionevole tentare di sfumare la netta distinzione tra pubblico e privato –, il timore è quello di dar vita ad approcci "iper-garantisti" che non tengono in debito conto le differenze tra le varie tipologie di dati reperibili in Rete. Come si avrà modo di osservare, le informazioni estrapolabili dai *social network* si caratterizzano per essere tanto variegate da richiedere al processualista di effettuare una o più classificazioni al fine di distinguere, anche nella realtà cibernetica, ciò che è pubblico, ciò che è riservato e ciò che è segreto.

---

[86] Cfr. Part I, Cap. II, par. 1.

[87] La considerazione è ripresa da G. SORCI, I social network. *Nuovi sistemi di sorveglianza e controllo sociale*, Palermo, 2015, p. 97.

[88] Testualmente, proprio con riguardo alle piattaforme *social*, S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 322.

[89] Sembra orientata in tal senso, ad es., F. IOVENE, *Le c.d. perquisizioni on line*, cit., p. 334-336. Nella letteratura straniera, v. L. ANDREWS, *I Know Who You Are and I Saw What You Did*, cit., p. 118, 135. Sul punto, però, si rivelano ancora di attualità, nel mantenere salde tali differenze, le riflessioni di F. CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, p. 9-24, 55-79.

[90] Si tratta di una tendenza che è possibile riscontrare anche in altri ordinamenti. A mero titolo esemplificativo, si pensi al "*derecho al proprio entorno virtual*", un diritto di nuova generazione sviluppatosi nella dottrina e nella giurisprudenza iberica, il cui obiettivo è quello di fornire una protezione ampia alla variegata tipologia di informazioni digitali contenute in un sistema informatico, comprese quelle generate dagli utenti dei *social network* (Tribunale Supremo spagnolo, 17 aprile 2013, n. 342).

All'opposto, va facendosi strada la propensione a liquidare frettolosamente come "pubblica" qualunque attività realizzata sui *social*, di talché nessun limite potrebbe essere opposto alle operazioni di acquisizione di dati sulle piattaforme digitali. Anche laddove le informazioni condivise in Rete assumano effettivamente il carattere *open access*, peraltro, si assume talvolta che la mera diffusione porti con sé un consenso implicito alla loro raccolta per finalità investigative.

Impostato in questi termini, il dibattito non può che portare a una polarizzazione del conflitto tra due visioni estreme che, in quanto tali, appaiono entrambe prive di ragionevolezza. Occorrerebbe, invece, tentare di valorizzare la *privacy* in maniera composita e ragionata, cercando di differenziare quelle attività intrusive effettivamente in grado di pregiudicare l'intimità della vita privata da quelle che non sembrano in alcun modo porsi in contrasto con tale esigenza.

In tal senso, si rivela di estrema utilità il riferimento all'art. 8 CEDU – nella parte in cui garantisce a ogni persona il diritto al rispetto della propria vita privata – e, specialmente, alla giurisprudenza della Corte di Strasburgo che ne ha delineato la portata, i confini e, di riflesso, l'ambito applicativo. Se è vero che, sotto il profilo qui in esame, la disposizione pattizia «si palesa più garantista della Costituzione italiana – ma non in contrasto con essa»[91], è proprio a quest'ultima che occorrerà riferirsi per cercare di individuare il campo di operatività della riservatezza nell'ambito delle piattaforme digitali. L'auspicio, come si cercherà di mettere in luce, è, ancora una volta, quello che «la contaminazione con la giurisprudenza di Strasburgo – sempre più autentica fonte del diritto processuale penale – possa condurre a realizzare un processo più giusto nella prassi quotidiana, per tutti i soggetti coinvolti»[92].

5. Il domicilio informatico: vecchi diritti, nuove tutele

L'espressione "domicilio informatico"[93] è ormai entrata nel vocabolario di base del processualpenalista del XXI secolo. Nata e sviluppatasi nel contesto del diritto penale sostanziale a seguito dell'introduzione della nuova fattispecie di cui all'art. 615-*ter* c.p.[94], la locuzione in parola è volta a descrivere e, di riflesso, tutelare quelle attività umane private realizzate nel *cyberspazio*, rispetto alle quali l'utente può vantare uno *ius includendi se* e uno *ius excludendi alios*.

Lo stretto legame che intercorre con la corrispettiva fattispecie analogica (si legga, il domicilio fisico[95]) è stato messo in luce, fin dal principio, dallo stesso legislatore che, nella

---

[91] A. PACE, *Metodi interpretativi e costituzionalismo*, in *Quaderni costituzionali*, 2001,1, p. 48.

[92] Con estrema efficacia, M. GIALUZ, *L'apertura al sistema convenzionale muta gli equilibri e i connotati del giusto processo*, in *Dir. pen. proc.*, 2014, p. 12.

[93] Come ricorda E.M. MANCUSO, *L'acquisizione dei contenuti* e-mail, cit., p. 512, nt. 45, la nozione di «domicilio informatico» va tenuta ben distinta da quella di «domicilio digitale», giacché con quest'ultima si intende, ai sensi dell'art. 1, comma 1, lett. *n-ter*) del d.lgs. 7 marzo 2005, n. 82, «l'indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito qualificato elettronico». A favore, invece, dell'irrilevanza lessicale, sembra mostrarsi S. SIGNORATO, *Le indagini* digitali, cit., p. 61.

[94] L. 23 dicembre 1993, n. 547.

[95] Come risaputo, vi è controversia in dottrina circa il significato da attribuire alla nozione costituzionale di domicilio. Secondo un primo orientamento, oggetto di tutela sarebbero esclusivamente i luoghi di privata dimora di cui all'art. 614 c.p. Altri autori, per converso, pur riconoscendo uno stretto legame tra il precetto costituzionale e la disposizione codicistica, adottano un approccio estensivo, inglobando nel concetto di

relazione di accompagnamento al nuovo delitto di «accesso abusivo ad un sistema informatico o telematico», ha qualificato i «sistemi informatici» alla stregua di «un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione». Ed è in questa medesima prospettiva, d'altro canto, che si inserisce l'elaborazione della Corte di cassazione in merito all'individuazione del bene giuridico tutelato all'art. 615-*ter* c.p.: il domicilio informatico è da intendersi «quale spazio ideale di esclusiva pertinenza di una persona fisica o giuridica, delimitabile prendendo come parametro il domicilio delle persone fisiche, ed al quale risulta estensibile la tutela della riservatezza della sfera individuale, che costituisce bene costituzionalmente protetto»[96]. Trattasi, in breve, di uno «spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona» che deve essere salvaguardato quale che sia il contenuto dei dati *ivi* racchiusi, purché attinenti alla «sfera di pensiero o all'attività lavorativa o non dell'utente»[97].

La trasposizione, nell'universo digitale, del concetto di domicilio, però, non ha convinto una parte della dottrina penalistica che, all'indomani dell'entrata in vigore della nuova ipotesi delittuosa, ha evidenziato come il richiamato parallelismo «colga solo parzialmente il contenuto dell'interesse all'esclusione di terzi da determinate "sfere di disponibilità e rispetto" create e rese fruibili dalla tecnologia informatica»[98]. La critica mossa al "nuovo" diritto fondamentale è di non aver compreso appieno che l'interesse dell'utente è quello di tutelare le proprie informazioni private o segrete, prescindendo dal luogo in cui esse si trovino e dal mezzo utilizzato[99].

L'esigenza di ricercare una tutela che si spinga al di là della sfera domestica spiega l'abbandono della categoria dogmatica "domicilio informatico" a favore della più ampia – ma, sotto certi aspetti, generica e impalpabile – "riservatezza informatica", definita dai suoi più convinti sostenitori come uno spazio virtuale di manifestazione della personalità nel quale l'utente è titolare di un «interesse esclusivo, giuridicamente riconosciuto, di godere, disporre e controllare le informazioni, i procedimenti, i sistemi e spazi informatizzati e le relative utilità»[100]. Dalle ceneri del domicilio informatico emerge, dunque, un diritto inedito in grado di tutelare le propaggini elettroniche della persona (*rectius*, lo *smartphone*) con le quali l'*Homo technologicus* «esprime le sue capacità professionali, culturali e più in

---

domicilio tutti quei luoghi nei quali è temporaneamente garantita un'area di intimità. Infine, non sono mancati tentativi di elaborare un'autonoma nozione costituzionale di domicilio, del tutto slegata dalla normativa penalistica. Cfr., per un quadro d'insieme, P. BARILE – E. CHELI, voce *Domicilio (libertà di)*, n *Enc. dir.*, vol. XIII, Milano, 1964, p. 861 ss.

[96] Così, Cass. pen., Sez. II, 14 gennaio 2019, n. 21987.

[97] Cass. pen., Sez. VI, 4 ottobre 1999, n. 3065.

[98] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Id., (a cura di), *Il diritto penale dell'informatica nell'epoca di* Internet, Padova, 2004, p. 53.

[99] F. IOVENE, *Le c.d. perquisizioni on line*, cit., p. 325. Nello stesso senso, P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. giust.*, 2016, p. 126.

[100] R. FLOR, Phising, identity theft *e* identity abuse. *Le prospettive applicative nel diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, p. 899; L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei* social network. *Aspetti penali*, in *Giur. mer.*, 2012, p. 2532, che parla di un «diritto di escludere terzi non autorizzati dall'accesso e dalla fruibilità di spazi, sistemi, dati informatici, a prescindere da loro contenuto "personale" o meno».

generale, le sue facoltà intellettive»[101], a prescindere dal luogo fisico ove questi sono ubicati (privata dimora, automobile, strade pubbliche, etc.). Si esplicita, in tal modo, quella connessione – identificata da tempo in dottrina[102] – tra la libertà domiciliare (analogica) e il diritto alla riservatezza: l'art. 14 Cost. è volto a tutelare sia lo *ius admittendi* ed *excludendi alios*, sia la prospettiva di preservare da interferenze esterne un'intangibile sfera di privatezza del cittadino[103].

Le considerazioni svolte fino ad ora assumono una certa consistenza anche sul versante processuale e, specialmente, con riguardo al tema oggetto di trattazione.

Il problema, in particolare, riguarda la necessità di individuare idonee garanzie costituzionali per far fronte ad attività investigative capaci di incidere sulla sfera privata del soggetto. Si pensi all'acquisizione, mediante sequestro del *device* o impiego del captatore informatico, di informazioni segrete e riservate contenute nei *social network*, come le *chat Whatsapp* o altri dati presenti nelle piattaforme digitali[104]. A tal proposito, occorre chiedersi se vi sia davvero la necessità di enucleare nuovi diritti o se, come sembra più ragionevole sostenere, sia sufficiente interpretare in maniera evolutiva ed estensiva le garanzie già enunciate dalla Carta Fondamentale.

Sul punto, come noto, ferve un acceso dibattito.

Già sul finire degli anni '80, la Corte costituzionale tedesca, nel riconoscere che i dispositivi elettronici avevano ormai assunto un'importanza fondamentale nello sviluppo della personalità umana, affermò l'esistenza di un nuovo diritto inviolabile all'autodeterminazione informativa[105], cioè la facoltà del singolo cittadino di poter governare autonomamente la cessione e il trasferimento dei propri dati personali. La medesima necessità di enucleare un *quid novi* rispetto al dettato costituzionale è emersa, più recentemente, nella storica sentenza con la quale i giudici tedeschi hanno identificato il «diritto alla segretezza e all'integrità dei sistemi informatici»[106], anch'esso un nuovo diritto fondamentale volto a proteggere, nel solco di una piena valorizzazione della dignità umana, l'interesse del cittadino a non subire indebite interferenze statali nei propri dispositivi elettronici, a prescindere dalla qualità o dalla quantità dei dati contenuti.

L'opera esegetico-creativa della Corte alsaziana[107], com'era forse prevedibile, non è passata inosservata nel panorama italiano, tanto che una parte della dottrina ha sentito la necessità di "spingersi oltre", consacrando un "nuovo" «diritto all'intangibilità della vita digitale»[108], in grado di offrire una tutela non tanto allo strumento informatico in sé, bensì

---

[101] Testualmente, con plastica efficacia, L. CUOMO, *La tutela penale del domicilio informatico*, in *Cass. pen.*, 2000, p. 2998.

[102] G. AMATO, sub *Art. 14 Cost.*, in G. Branca (a cura di), *Commentario alla Costituzione*, Bologna-Roma, 1977, p. 57 ss.; A. PACE, *Problematica delle libertà fondamentali*, cit., p. 197.

[103] Corte cost., 16 maggio 2008, n. 149. In termini non dissimili, v. Corte cost., 24 aprile 2002, n. 135. Tanto è vero che in dottrina si è esplicitamente affermato che il domicilio sarebbe, in realtà, un bene strumentale alla tutela della vita privata dell'individuo (F. CAPRIOLI, *Colloqui riservati e prova penale*, cit., p. 57).

[104] Cfr. Parte II, Cap. V.

[105] Bundesverfassungsgericht, 15 dicembre 1983 n. 65.

[106] Bundesverfassungsgericht, 27 febbraio 2008 n. 370.

[107] …che è nuovamente intervenuta sul punto con la pronuncia Bundesverfassungsgericht, 1 BvR 966/09, 1 BvR 1140/09, 20 aprile 2016

[108] L'intuizione si deve a S. SIGNORATO, *Le indagini digitali*, cit., p. 70.

all'individuo che ne risulta titolare. Si è al cospetto, in buona sostanza, di una sorta di "macrodiritto" estremamente dinamico volto a tutelare non solo il domicilio, ma anche la vita privata, nonché la libertà e la segretezza delle comunicazioni[109].

A fronte di queste nuove e numerose elaborazioni dottrinali e giurisprudenziali ("riservatezza informatica", "intangibilità della vita digitale", etc.), però, altri autori hanno fatto notare come non sia agevole individuare il referente costituzionale, tanto che, in molti casi, sembrerebbe doversi richiamare la clausola contenuta nell'art. 2 Cost., la quale, come si è detto, consente – secondo una certa corrente di pensiero – di tutelare quei valori di libertà emergenti con il passare del tempo. Si è al cospetto, però, di una disposizione, quest'ultima, che non garantisce i medesimi livelli di tutela (riserva di legge e riserva di giurisdizione) previsti agli artt. 13 ss. Cost., a meno di non voler (condivisibilmente) richiamare il presidio contenuto all'art. 8 CEDU[110]. L'ingerenza statale nel diritto al rispetto della vita privata, come si è già detto, può avvenire solo nel rispetto di determinati presupposti e condizioni: la limitazione deve essere prevista dalla legge (*i*), necessaria e proporzionale in una società democratica (*ii*), finalizzata al perseguimento di uno scopo legittimo tra quelli espressamente enunciati dalla Carta (*iii*) e vagliata da un organo autonomo e indipendente (*iv*).

Nell'era tecnologica, dunque, è certamente comprensibile l'esigenza di mettere a punto nuove categorie giuridiche e, tra queste, veri e propri diritti fondamentali. Ciò nondimeno, occorre chiedersi se sia sempre necessario ricorrere a tali elaborazioni o se, quando possibile, non sia più opportuno, per esigenze di maggior tutela, cercare di individuare, piuttosto, nuove declinazioni dei diritti tradizionali[111].

È quest'ultima, a ben riflettere, la via che andrebbe perseguita, perlomeno qualora il testo costituzionale lo consenta, come nel caso del domicilio informatico[112].

A fronte di chi ritiene si tratti di «nuova categoria concettuale» ricavabile dall'art. 2 Cost.[113], altri autori ne sostengono, per contro, la natura non inedita e, di riflesso, la piena riconducibilità all'art. 14 Cost.; una disposizione, quest'ultima, che, nel contesto di una società in continuo movimento, si apre a «nuove forme di tutela» o, meglio, a meri «aggiornamenti e ridefinizioni» della libertà fondamentale *ivi* enunciata[114].

A sconfessare quest'ultima impostazione, però, soccorrerebbe un dato all'apparenza insuperabile: la disposizione costituzionale tutelerebbe gli individui solo a fronte di

---

[109] S. SIGNORATO, *Le indagini digitali*, cit., p. 69.

[110] La necessità di richiamare l'art. 2 quale base giuridica per tutelare la riservatezza informatica, ma in combinato congiunto con l'art. 8 CEDU, è sostenuta da F. IOVENE, *Le c.d. perquisizioni on* line, cit., p. 336.

[111] Autorevole dottrina, del resto, ha messo in luce, benché in una prospettiva più generale, la necessità di affrontare le nuove sfide poste dall'evoluzione tecnologica tenendo in debito «conto anche della possibilità di ritenere comprese nelle già esistenti garanzie costituzionali le nuove modalità d'azione offerte dalla rete» (S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 384).

[112] Nella medesima linea di pensiero sembrerebbero porsi anche F. CENTORAME, *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. it. dir. proc. pen.*, 2021, p. 518; M. MIRAGLIA, *Il "*Trojan *(non) di Stato": una disciplina da completare*, in *Proc. pen. giust.*, 2023, p. 1237.

[113] R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen.*, 2018, p. 543.

[114] È l'opinione sostenuta, ad es., da G. SILVESTRI, *L'individuazione dei diritti della persona*, cit., p. 3 s.

un'«intrusione fisica» nel domicilio[115]. Di conseguenza, il *cyberspazio*, in quanto luogo fittizio e, dunque, "non-luogo", non potrebbe essere ricondotto nella sfera di garanzia dell'art. 14 Cost. Del resto, si è altresì osservato come appaia «scorretto invocare, per l'utilizzo del *computer*, l'art. 14 Cost. […] posto che la libertà di domicilio "presuppone" la separatezza "fisica" del luogo»[116] e, di conseguenza, la realizzazione di comportamenti esteriormente percepibili.

In realtà, la "fisicità" non sembra essere un carattere imprescindibile ai fini della tutela prevista dalla norma costituzionale, perlomeno per un duplice ordine di ragioni.

In primis, le limitazioni previste al secondo comma della disposizione (ispezioni, perquisizioni e sequestri[117]), a differenza di quanto sostenuto in passato[118], possono essere oggi esercitate anche in spazi virtuali, posto che il legislatore del 2008 ha espressamente individuato specifiche forme di "intrusioni informatiche" (artt. 244, comma 2; 247, comma 1-*bis*; 254-*bis* c.p.p.).

In secundis, la dottrina più attenta ha osservato come il concetto di "luogo" possa essere agevolmente esteso tanto ai supporti informatici, quanto a ogni ambiente virtuale, giacché tale locuzione dev'essere interpretata come «spazio potenzialmente idoneo a contenere qualcosa»[119] e, pertanto, financo i *bit* digitali. A conclusioni non dissimili, peraltro, potrebbe giungersi facendo leva su un concetto ibrido di "spazio" inteso, cioè, come luogo fisico nel quale si trovano le strumentazioni e i "nodi" della Rete e, contestualmente, come luogo digitale generato e formato da dati e da questi ultimi incessantemente alimentato[120]. L'*argomentum*, d'altro canto, sembra essere confermato da una recente pronuncia della Suprema corte che, chiamata a giudicare in merito all'estensione dell'art. 615-*ter* c.p., ha espressamente inglobato le piattaforme *Cloud* (nel caso di specie, *Dropbox*) nella nozione di domicilio informatico tutelata all'art. 14 Cost.[121].

A sostengo dell'esegesi evolutiva ed estensiva qui sostenuta milita, ancora, un ulteriore, fondamentale e dirimente considerazione.

---

[115] È questa la tesi prospettata da R. ORLANDI, *Osservazioni sul documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Arch. pen.* web, 25 luglio 2016, p. 1, da cui è tratta la citazione. Concordi, F. IOVENE, *Le c.d. perquisizioni on* line, cit., p. 336, per la quale in ambito digitale «non ci sono confini, non ci sono luoghi fisici che possano riflettere il carattere privato o riservato delle attività che ivi si svolgano o di ciò che vi sia custodito»; P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale*, cit., p. 126.

[116] A. PACE, *Metodi interpretativi*, cit., p. 55, nt. 76.

[117] È noto il dibattito relativo alla corretta individuazione dei limiti alla libertà di domicilio. La dottrina maggioritaria, a fronte di un'impraticabilità dell'estensione analogica del testo costituzionale, propende per un'interpretazione letterale, tale per cui la limitazione del domicilio può avvenire solo per causa di uno o più atti tipizzati dall'art. 14, comma 2, Cost. (in tal senso, v. L. FILIPPI, *L'intercettazione di comunicazioni*, cit., p. 55-59; A. PACE, *Problematica delle libertà costituzionali*, cit., p. 223). La giurisprudenza costituzionale, al contrario, adotta un'impostazione meno rigorosa, ammettendo anche l'impiego di strumenti di compressione della libertà *de qua* non tipizzati, sul presupposto che i Padri Costituenti non avrebbero potuto «tener conto di forme di intrusione divenute attuali solo per effetto dei progressi tecnici successivi» (Corte cost., 24 aprile 2002, n. 135).

[118] A. PACE, *Metodi interpretativi*, cit., p. 55, nt. 76.

[119] L'intuizione è di S. SIGNORATO, *Le indagini* digitali, cit., p. 57-61.

[120] Su tale "doppio" carattere di *Internet*, v. A. PAPA, *Espressone e diffusione del pensiero in* Internet, cit., p. 34 s.

[121] Cass. pen., Sez. V, 22 febbraio 2023, n. 27900.

Se la *ratio* originaria e il nucleo essenziale dell'art. 14 Cost. si identificano con la necessità di tutelare quello spazio (fisico) nel quale si proiettano le plurime dimensioni (individuali e relazionali) della persona[122] nella «prospettiva di preservare da interferenze esterne comportamenti tenuti in un determinato ambiente»[123], non si comprende perché mai tale protezione non potrebbe essere estesa anche alle proiezioni informatiche dell'individuo[124]. A ben vedere, infatti, l'esigenza di garantire la sfera intima e riservata della persona si manifesta, nell'attuale epoca digitale, anche e soprattutto in ambienti virtuali. È pur vero – si dirà – che il Costituente quando ha redatto l'art. 14 Cost. si era posto nella prospettiva di tutelare il bene fisico del domicilio; ma, a ben riflettere, restringere oggi tale concetto alla mera dimensione analogica è espressione di un reflusso "originalista" che mal si adatta alle sfide poste dalla nuova realtà digitale. Mette conto osservare, peraltro, come l'esigenza di interpretare in maniera quanto più estensiva le norme costituzionali istitutive di diritti fondamentali derivi, senza mezzi termini, dal pieno riconoscimento del già richiamato "principio di massima espansione delle libertà".

Ciò che rileva, dunque, ai fini dell'operatività dell'art. 14 Cost. non è tanto il "luogo", fisico o virtuale, bensì, come si è cercato di dimostrare, la necessità di salvaguardare il carattere intimo e privato delle attività realizzate dall'individuo[125]; un'esigenza, quest'ultima, che deve ritenersi sussistente pure in relazione alle mansioni di vita quotidiana realizzate *on the web*.

A nulla varrebbe obiettare, peraltro, la difficoltà nel qualificare un luogo digitale alla stregua di un domicilio informatico sul presupposto che quest'ultimo non potrebbe essere visto come un luogo abitativo o uno spazio nel quale si svolge la propria attività lavorativa; requisiti, questi ultimi, che concorrerebbero a delineare il concetto di domicilio. È noto, infatti, che la giurisprudenza di legittimità e la dottrina più accreditata[126] abbiano accolto una nozione sufficientemente estesa della locuzione in parola, intesa, cioè, quale luogo funzionalmente deputato allo «svolgimento di manifestazioni di vita privata […] in modo riservato ed al riparo da intrusioni esterne»[127], tra le quali vengono ricomprese attività ulteriori rispetto a quelle lavorative o *stricto sensu* domestiche[128].

---

[122] L'elaborazione della concezione del domicilio come «proiezione spaziale» si deve, come noto, ad A. AMORTH, *La Costituzione italiana. Commento sistematico*, Milano, 1948, p. 62.

[123] Corte cost., 11 aprile 2002, n. 135, la quale riprende la nozione di domicilio offerta da P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., p. 154, che parla di una «sfera spaziale volta a preservare il carattere "privato" di determinati comportamenti soggettivi».

[124] Sembra suggerire un approccio di questo tipo F. CAPRIOLI, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, in L. Lupária – L. Marafioti – G. Paolozzi (a cura di), *Dimensione tecnologica e prova penale*, Torino, 2019, p. 49, il quale soggiunge come «lavorare sulle potenzialità espansive dell'art. 14 Cost. sia meno rischioso che affidarsi agli incerti confini del diritto al rispetto della vita privata e ai mutevoli umori della Corte europea» (p. 51). Del «sistema informatico» come «propaggine della propria mente» parlava, già, G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, p. 523.

[125] Cfr., tra le molte, Corte cost., 16 maggio 2008, n. 149, cit.

[126] A. PACE, *Problematica delle libertà costituzionali*, cit., p. 214.

[127] Cass. pen., Sez. Un., 28 marzo 2006, n. 26795.

[128] Tra le manifestazioni della vita privata realizzabili nel domicilio, difatti, vengono espressamente ricomprese anche il riposo, lo svago, l'alimentazione, lo studio, le attività professionale e di lavoro (in questi termini, Cass. pen, Sez. Un., 23 marzo 2017, n. 31345). Nello stesso senso, v. la Relazione alla proposta di legge C. 4260 (primo firmatario l'on. Quintarelli) depositata alla Camera dei deputati in data 31 gennaio 2017 (Modifiche al codice di procedura penale e altre disposizioni concernenti la disciplina dell'intercettazione di

Allo stesso modo, non pare ragionevole svilire la portata innovativa e garantista del concetto di domicilio informatico escludendo la sua violazione ogniqualvolta il dispositivo contenente i *bit* digitali si trovi al di fuori di una privata dimora. L'assunto, prospettato da una certa giurisprudenza[129], non tiene conto del fatto che il bene giuridico in esame è oggetto di tutela «*ex se* a prescindere dal luogo in cui viene custodito»[130]. Poco importa, dunque, la collocazione fisica del *device*; ciò che conta davvero è che le informazioni siano contenute in uno spazio virtuale rispetto al quale il titolare può legittimamente vantare uno *ius excludendi alios*.

In conclusione, il domicilio informatico, lungi dall'essere una categoria incompleta e imperfetta, sembra poter offrire ampi margini di tutela a fronte di attività a carattere tecnologico connotate da un'elevata intrusività. Va così emergendo un concetto di domicilio «proiettato verso nuove dimensioni "tecnologiche"»[131] e, dunque, in grado di tutelare appieno anche quegli spazi virtuali nei quali la persona svolge quotidianamente le proprie attività. Del resto, se è vero, come ebbe a osservare uno dei Padri fondatori della *privacy* nella storica *dissenting opinion* resa nel caso *Olmstead c. Stati Unti*[132], che «*advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions*», può mai essere che la Carta Fondamentale non garantisca alcuna protezione contro una tale invasione?

Il riconoscimento di un concetto ampio e aggiornato di domicilio, però, non rappresenta certo la panacea contro tutti i mali delle "indagini penali 2.0". È evidente, infatti, che lo studioso, qualora l'operazione investigativa non implichi in alcun modo la limitazione della libertà domiciliare (come, ad esempio, nel caso di acquisizione di informazioni pubbliche[133]), debba trovare altre vie per tutelare, ove necessario, i diritti fondamentali dell'indagato e dei terzi eventualmente coinvolti dalla misura.

---

comunicazioni telematiche e dell'acquisizione di dati ad esse relativi), nella quale il domicilio informatico è definito come «quello spazio immateriale, delimitato da informazioni, nel quale una persona esplica attività legate alla vita privata o di relazione, e dall'accesso al quale il titolare ha diritto di escludere terzi».

[129] Cass. pen., Sez. V, 14 ottobre 2009, n. 16556.

[130] M. TROGU, *Intrusioni segrete nel domicilio informatico*, in A. Scalfati (a cura di), *Le indagini atipiche*, cit., p. 587.

[131] M. MONTAGNA, *Libertà domiciliare*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*, Milano, 2019, p. 148, la quale pare condividere la tesi diretta ad ancorare la tutela del domicilio informatico al dettato dell'art. 14 Cost.

[132] Cfr. Parte I, Cap. I, par. 4.

[133] Cfr. Parte II, Cap. II e III. Anche nell'ambiente digitale, del resto, è possibile disquisire di «*'public areas' or 'public access areas'*», onde per cui il nuovo concetto di domicilio informativo «*is unable to offer a comprehensive 'shield' in which the data subject can effectively enjoy her right to exclude others from the access to her data*» (così, S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020, p. 61). Più in generale, tuttavia, manifestano dubbi in merito all'effettiva capacità della nozione di domicilio informatico di soddisfare a pieno le esigenze di tutela del dato digitale nell'attuale realtà fenomenica, L. BARTOLI – G. LASAGNI, *The handling of digital evidence in Italy*, in M. Caianiello – A. Camon (a cura di), *Digital forensic evidence. Towards common european standards in antifraud administrative and criminal investigation*, Padova, 2021, p. 88; S. QUATTROCOLO, *Qualcosa di meglio del diritto (e del processo) penale?*, cit., p. 172.

CAPITOLO II

LE INDAGINI SU "FONTI PUBBLICAMENTE ACCESSIBILI" NEL PANORAMA ITALIANO: IL *SOCIAL NETWORK PATROLLING*

SOMMARIO: 1. "Dati pubblici", "dati non pubblici" e "altri dati": l'eterogeneità delle informazioni ricavabili dai *social network*. – 2. La nozione di "fonte pubblicamente accessibile" nel contesto delle nuove forme di comunicazione digitale. – 3. Alle origini del cd. *cyberpatrolling*: sorveglianza di massa, controllo individualizzato e SOCMINT. – 3.1 Il *social network patrolling*: una nuova frontiera investigativa. – 3.2 *Cyberpatrolling* e società del controllo: lo Stato vigilante nell'era della cd. *coveillance*. – 4. Il campo d'azione del "pattugliamento virtuale": *intelligence*, prevenzione e repressione criminale. – 5. Servizi segreti e vigilanza continuativa: alla ricerca di un ragionevole equilibrio. – 6. "Ronde poliziesche virtuali" e prevenzione dei reati. – 6.1 Sorveglianza nei *social network* e pre-inchiesta: l'art. 330 c.p.p. come limite allo svolgimento di operazioni investigative *online* lesive del diritto alla riservatezza. – 6.2 Le *open source information* ricavate dai *social network* tra attività di *predictive policing* e tecnologie di riconoscimento facciale. – 7. *Social network mining* e indagini preliminari. – 7.1 La veste giuridica del *cyberpatrolling* investigativo e l'(in)utilizzabilità delle informazioni raccolte. – 7.2 Alla ricerca della legalità perduta… o meglio, mai esistita. – 8. L'acquisizione transfrontaliera delle informazioni pubblicamente disponibili nei *social-accounts*: i nuovi scenari della *jurisdiction to investigate*. – 8.1 L'art. 32, comma 1, lett. a), della Convenzione di Budapest sul crimine informatico: il concetto di "fonte pubblica" nelle ipotesi di *transborder access*. – 8.2 La libera accessibilità ai dati *open source* ubicati in territorio straniero: profili critici dell'art. 234-*bis* c.p.p.

1. "Dati pubblici", "dati non pubblici" e "altri dati": l'eterogeneità delle informazioni ricavabili dai *social network*

«Vi fu un momento, nella nostra storia, in cui tutte le attività del cittadino comune si trasformarono in dati, e quel momento è chiaramente correlato all'avvento e al successo planetario dei cosiddetti *social network*»[1]. Con queste parole, accreditata dottrina ha efficacemente sottolineato uno degli aspetti più significativi legati all'impiego delle nuove piattaforme digitali come strumenti di comunicazione e partecipazione alla vita pubblica: la produzione bulimica, incessante e durevole di dati.

Come si è già osservato, le numerose interazioni sociali realizzate in Rete tramite la condivisione da parte degli utenti di contenuti digitali (si pensi, ad esempio, a documenti, video, immagini, foto, commenti, azioni di auto-geolocalizzazione, etc.[2]) ha generato un flusso massiccio e continuo di informazioni. Il fenomeno, plasticamente descritto in termini di «*datafication*» (cioè, «*transformation of social action into online quantified data*»[3]), ha reso i *social network* la più grande banca dati attualmente esistente.

[1] G. ZICCARDI, *Diritti digitali. Informatica giuridica per le nuove professioni*, Milano, 2022, p. 54.

[2] Per una rassegna, v. S. BARRERA, *Claves de la Investigaciòn en Redes Sociales*, Roquetas de Mar, 2016, p. 237.

[3] Il concetto, e la relativa definizione, sono riprese da V. MAYER-SCHÖNBERGER – K. CUKIER, *Big data. A Revolution That Will Transform How we Leave, Work and Think*, Oxford, 2014, p. 179, i quali soggiungono come la locuzione *de qua* si riferisca, più in generale, alla «*ability of networked platforms to render into data many aspects of the world that have never been quantified before*».

Sennonché, le informazioni che possono essere ricavate da questi siti *web* risultano a tal punto variegate ed eterogenee (nel linguaggio informatico, "non strutturate") da rendere di fatto impossibile una compiuta classificazione delle stesse, sotto il profilo sia qualitativo sia quantitativo[4]. Ciò nondimeno, lo studio del concreto funzionamento dei suddetti strumenti di comunicazione consente di distinguere due macrocategorie, utili a orientarsi nello studio di una tematica in costante evoluzione: "dati pubblici" (*i*) e "dati non pubblici" (*ii*).

Nel primo gruppo (*i*) possono ricomprendersi tutte quelle informazioni che l'utente inserisce direttamente nella piattaforma senza apporre alcuna chiave di protezione, rendendole così disponibili e fruibili a chiunque vi abbia interesse. Ponendo mente a *Instagram*, si può fare l'esempio di un profilo "aperto" nel quale ciascun utente della Rete è abilitato a visualizzare i contenuti sullo stesso caricati. Si tratta, come dimostrano l'analisi empirica e le ricerche scientifiche[5], di un'ipotesi molto frequente, posto che la maggior parte degli utilizzatori dei *social network* – specialmente se di giovane età – non ritiene di dover adottare determinate impostazioni di *privacy*; del resto, una simile limitazione – viene comunemente affermato– si porrebbe in contrasto con l'idea stessa di "rete sociale", un universo nel quale lo *sharing* di notizie e informazioni rappresenta la stessa ragion d'essere della piattaforma[6].

All'interno della categoria dei "dati pubblici", in realtà, occorre ulteriormente distinguere a seconda che la pagina *social* sia accessibile solo ed esclusivamente agli utenti iscritti alla medesima piattaforma ovvero a chiunque abbia la possibilità di connettersi a *Internet*. *LinkedIn*, ad esempio, ha recentemente messo a disposizione dei propri utenti una particolare funzionalità *privacy* che consente di rendere visibile il proprio *account* solo a coloro che fanno parte della medesima "rete sociale"[7].

Al contrario, nella seconda classe (*ii*) devono annoverarsi, alla luce di un criterio di residualità, tutti quei dati che non sono pubblicamente accessibili. Trattasi, com'è intuibile, di una categoria eterogena, potendo racchiudere in sé informazioni rispetto alle quali vi è una totale assenza di pubblicità – intesa come astratta conoscibilità in capo a una platea

[4] Per un'esemplificazione (indubbiamente non esaustiva) delle numerose informazioni ricavabili dai *social network sites*, v. J. GRIMMELMANN, *Saving Facebook*, in *Iowa Law Review*, 2009, p. 1137 ss. e, spec., p. 1149 ss.

[5] J.P. SEMITSU, *From facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Government Surveillance*, in *Pace Law Review*, 2011, p. 319 e, in part., nt. 85.

[6] A tal proposito, i più attenti commentatori hanno osservato che «*Facebook* non è solo un sito *web*. È un ecosistema che induce i suoi abitanti a condividere informazioni personali e rivelare i pensieri più intimi» (così, nuovamente, J.P. SEMITSU, *From facebook to Mug Shot*, cit., p. 293, trad. nostra). Non è un mistero, del resto, che le piattaforme di comunicazione siano progettate – si pensi, ad esempio, all'impiego dell'algoritmo che supervisiona la funzionalità "*News Feed*" – in modo tale da manipolare surrettiziamente la volontà degli individui affinché questi siano indotti a divulgare informazioni che altrimenti manterrebbero riservate (cfr. A.E. WALDMAN, *Privacy, Sharing, and Trust: The Facebook Study*, in *Case Western Reserve Law Review*, 2016, p. 193 ss., e, spec., p. 223 ss.).

[7] Rientrano in questa categoria, salvo diversa impostazione di *privacy*, anche i messaggi, i cd. *tweet*, che l'utente condivide nel proprio profilo *Twitter*. Ciò significa che il loro contenuto può essere visualizzato non solo da parte dei *followers*, ma anche dalla totalità dei naviganti del *web* (A. RODRÍGUEZ ÁLVAREZ, *Proceso penal y twitter: manual de instrucciones*, in *Propostas de modernización do dereito*, diretto da M. García Goldar – J. Ammerman Yebra, Santiago de Compostela, 2017, p. 115).

indeterminata e indefinita di soggetti[8] –, ovvero una conoscibilità limitata, come nell'ipotesi in cui l'utente abbia reso visibile il proprio profilo solo a una cerchia ristretta di utenti iscritti alla medesima piattaforma (cd. "amici" o *followers*).

Tanto premesso, non è affatto agevole, in concreto, riuscire ad allocare correttamente la singola informazione nell'ambito dell'una o dell'altra categoria.

Nell'era digitale e, più in particolare, nell'ambito dei *social network*, il confine tra pubblico e privato appare più che mai fluido, malleabile e in continuo movimento, dando vita a una "zona grigia" difficilmente riconducibile alle tradizionali categorie giuridiche e sociali[9]. Si consideri, in via esemplificativa, proprio l'ipotesi da ultimo ricordata nella quale un utente abbia impostato un livello di sicurezza del profilo tale da rendere visibili le proprie attività *online* esclusivamente a una cerchia ristretta di individui ("amici" o "amici di amici").

La riducibilità del dato a una (*i*), piuttosto che all'altra categoria (*ii*), è gravida di conseguenze sul piano processuale: a seconda della natura "pubblica", "non pubblica" o "ristretta" mutano le garanzie costituzionali di contesto e, di riflesso, le possibili modalità di ricerca e apprensione del materiale probatorio. Si pensi al problema di stabilire se, in un caso come quello appena evocato, le informazioni – non aventi carattere pubblico, né, tantomeno, privato, bensì «ristretto»[10] – possano essere legittimamente e liberamente apprese da chiunque (e, perciò, anche dalle autorità di *law enforcement* o dagli agenti di polizia giudiziaria) ovvero solo da soggetti a tale scopo autorizzati, come gli "agenti segreti attrezzati per l'inganno", cioè soggetti istituzionali che, utilizzando profili di copertura, inducono il bersaglio a farsi accettare nella propria cerchia di amici, al fine di acquisire informazioni altrimenti inaccessibili[11].

2. La nozione di "fonte pubblicamente accessibile" nel contesto delle nuove forme di comunicazione digitale

Avendo quale punto di riferimento la classificazione di massima sopra proposta, lo studio condotto in questa parte della trattazione avrà ad oggetto le modalità attraverso le quali le diverse autorità (tanto in fase di prevenzione, come in fase di repressione) possono visualizzare, acquisire e trattare, per finalità investigative e probatorie, dati e informazioni pubblicamente disponibili sui *social network*[12].

---

[8] Si pensi ai messaggi scambiati nella *chat* di *WhatsApp* o ai commenti privati alle *stories* pubblicate su *Instagram*.

[9] In proposito, parlano di un vero e proprio «*tertium genus*» tra dati pubblici e dati non pubblici, A. NIETO MARTIN – M. MAROTO, *Redes sociales en internet y "data mining" en la prosepcciòn e investigaciòn de comportamientos delictivos*, in *Revista de derecho penal y criminologia*, 2013, p. 47.

[10] È il termine comunemente utilizzato in dottrina per descrivere questo tipo di informazione (v., ad es., C. CONTI – M. TORRE, *Spionaggio digitale nell'ambito dei* social network, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 548; C. WARKEN, *Classification of Electronic Data for Criminal Law Purposes*, in *Eucrim*, 2018, 4, p. 1). Talvolta, nel contesto nordamericano, si ricorre anche all'impiego dell'espressione «*quasi-private information*» o «*quasi-private communication*» (cfr., rispettivamente, E. NORTH, *Facebook Isn't Your Space Anymore: Discovery af Social Networking Websites*, in *Kansas Law Review*, 2010, p. 1288 e L.M. GLADYSZ, *Status Update: When Social Media Evidence Enters the Courtroom*, in *Journal of Law and Policy for the Information Society*, 2012, p. 715).

[11] Il tema verrà trattato nella Parte II, Cap. IV.

[12] La prospettiva adottata in questa sede individua quale punto privilegiato dell'analisi non tanto il "luogo virtuale" nel quale l'informazione viene a collocarsi, bensì la sua accessibilità. Del resto, in un mondo

Prima di procedere in tale senso, però, è opportuno muovere da una premessa di carattere terminologico: a che cosa ci si riferisce, nell'ambito delle moderne piattaforme di comunicazione, quando si allude al concetto di *open access data* (dati pubblici)? Il quesito, a ben riflettere, chiama alla mente il noto dilemma di Sant'Agostino riferito a quei concetti della realtà immediatamente e comunemente percepiti dall'uomo, ma la cui essenza è difficile da spiegare[13]. In effetti, non è agevole individuare i tratti fondamentali che contribuiscono a connotare il carattere "pubblico" di un dato digitale, specialmente se riferito alle informazioni estrapolabili dai *social network*.

Si proceda con ordine.

Innanzitutto, deve darsi conto dell'impossibilità, allo stato attuale, di rintracciare una definizione normativa, ufficiale e condivisa di *open source data*. Benché numerose fonti sovranazionali (tanto di *hard law*, quanto di *soft law*) ricorrano frequentemente a tale espressione, nessuna di queste ne offre una compiuta esegesi. Si prenda, ad esempio, l'art. 32, comma 1, lett. a), della Convenzione di Budapest sul *cybercrime*[14], il quale si riferisce alle informazioni *open source* come a quelle «disponibili al pubblico (fonti aperte)», senza però fornire alcuna specificazione ulteriore.

A fronte di tale vuoto normativo, la letteratura in materia tende generalmente a stabilire un'equivalenza tra "pubblicità" e "libera accessibilità" (o "libera disponibilità") del dato[15].

In realtà, com'è stato recentemente messo in luce dal Garante per la protezione dei dati personali nell'ambito del trattamento delle informazioni in materia commerciale, occorre tenere ben distinte le "fonti pubbliche" dalle "fonti pubblicamente e generalmente accessibili"[16]. Nel primo caso, trattasi di notizie che ciascun cittadino può apprendere senza alcuna restrizione, ma solo dopo aver avanzato una specifica richiesta agli organi competenti in base alla normativa di riferimento[17]. Viceversa, nella seconda classe possono essere

---

cibernetico nel quale i dati digitali sono in costante movimento, non sembra opportuno continuare a ragionare utilizzando categorie dogmatiche nate e pensate per il "mondo fisico". I concetti di "luogo pubblico", "luogo aperto al pubblico", "luogo di privata dimora", "luogo riservato", etc. mostrano, nel contesto dei *social network*, tutta la loro fragilità. Emblematica, in tal senso, la "confusione" interpretativa sorta in seno alla giurisprudenza di legittimità in merito alla qualifica più opportuna da attribuire a *Facebook*: luogo pubblico, luogo aperto al pubblico o *tertium genus*? (cfr. Cass. pen., Sez. II, 25 marzo 2014, n. 37757, secondo cui la piattaforma *de qua* dovrebbe essere qualificata come una «piazza immateriale che consente un numero indeterminato di accessi e di visioni che può essere assimilat[a] al luogo pubblico»; Cass. pen., Sez. I, 12 settembre 2014, n. 37596, ove si riferisce a *Facebook* come a un «luogo aperto al pubblico»; Cass. pen., Sez. V, 1° marzo 2016, n. 8328). Più in generale, sulla difficoltà di inquadrare i nuovi *socia media* nel contesto delle tradizionali categorie dogmatiche articolate sulla distinzione luogo pubblico-luogo privato, v. L.B. LIDSKY, *Public Forum 2.0*, in *Boston University Law Review*, 2011, p. 1975 ss.

[13] «Che cos'è il tempo? Se nessuno m'interroga, lo so; se volessi spiegarlo a chi m'interroga, non lo so».

[14] Convenzione del Consiglio d'Europa sulla criminalità informatica, 23 novembre 2001.

[15] F. BUENO DE MATA, *Investigación y prueba de delitos de odio en Redes Sociales: Técnicas OSINT e inteligencia policial*, Valencia, 2023, p. 85, 123.

[16] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali*, 12 giugno 2019.

[17] L'art. 4, lett. a), *Codice di condotta per il trattamento dei dati personali*, cit., ricomprende in tale categoria il «registro delle imprese, i bilanci e gli elenchi dei soci, le visure e/o gli atti camerali». Nello stesso senso, peraltro, si esprime anche l'art. 3, comma 1, lett. j) del Codice della *privacy* spagnolo (*Ley Orgánica* 13 dicembre 1999, n. 15), laddove definisce le «*fuentes accesibles al público*» come «*aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación*».

annoverate tutte quelle informazioni liberamente accessibili, in via diretta e immediata, da parte di chiunque (soggetto pubblico o privato), tra le quali il Garante annovera espressamente anche i «siti *Internet*»[18].

La distinzione, del resto, era già stata colta dal legislatore italiano in fase di redazione del codice dell'Amministrazione Digitale[19], utile cartina al tornasole ogniqualvolta si debbano esaminare questioni di carattere tecnologico nell'ambito penalprocessuale. Nella versione originaria[20], l'art. 1, comma 1, lett. n), definiva il «dato pubblico» come quell'informazione «conoscibile da chiunque» e la «disponibilità» del dato (lett. o) in termini di «possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge».

Il *discrimen* tracciato dal provvedimento del garante e dall'atto normativo appena citato, pertanto, sembra giustificare un'interpretazione volta a ricomprendere nel concetto di *open access data* pure le informazioni liberamente accessibili nei *social network*, come, ad esempio, i dati contenuti nei profili pubblici di *Facebook*.

Muovendosi in queste coordinate teoriche, un'analisi sistematica delle principali fonti normative e dottrinali consente di individuare i criteri generalmente utilizzati per qualificare un'informazione come *publicly avaiable* nel contesto delle piattaforme di *sharing*: a) libero accesso da parte di chiunque vi abbia interesse, senza una necessaria autorizzazione preventiva o l'intermediazione di un terzo[21]; b) assenza di vincoli di proprietà (ad eccezione del diritto d'autore)[22]; c) assenza di «*sensitive contacts*»[23]; d) assenza di misure o sistemi di sicurezza atte a limitarne l'accesso.

Mentre i criteri *sub* a) e b) non pongono particolari problemi interpretativi, i restanti parametri, al contrario, richiedono qualche ulteriore riflessione.

In base alle impostazioni di *privacy* previste nei singoli *social web*, ogni utente può scegliere di condividere determinate informazioni esclusivamente con una cerchia ristretta di soggetti o solo all'interno di determinati "gruppi chiusi" (trattasi delle ipotesi di cd. *Friends-lock*). In questo caso, si realizza una *audience restriction* dell'accesso alle informazioni che non consente di classificarle come "pubbliche". È ben vero – si obietterà – che le stesse potrebbero, comunque, circolare liberamente nel ciberspazio a seguito di una ri-condivisione da parte di coloro che ne hanno la legittima disponibilità, ma ciò, in ogni caso, non autorizza a catalogarle come *publicly available*, almeno fino a quando non vengano inserite su pagine a libero accesso[24]. Di conseguenza, pare che il requisito *sub* c)

---

[18] Art. 4, lett. b), *Codice di condotta per il trattamento dei dati personali*, cit.

[19] D.lgs. 7 marzo 2005, n. 82.

[20] D.lgs. 26 agosto 2016, n. 179 recante modifiche ed integrazioni al Codice dell'amministrazione digitale, il cui art. 1, lett. h), ha disposto la soppressione, tra le altre, delle lettere delle lettere n) e o), dell'art. 1 del d.lgs. 7 marzo 2005, n. 82.

[21] Su questo specifico requisito, v. I. WALDEN, *Computer Crimes and Digital Investigations*, Oxford, 2007, p. 256. Cfr. anche N. SEITZ, *Transborder Search: A New Perspective in Law Enforcement?*, in *Yale Journal of Law and Technology*, 2005, p. 24.

[22] D. TROTTIER, *Coming to Terms with Social Media Monitoring. Uptake and Early Assessment*, in *Crime Media Culture*, 2015, p. 531.

[23] Così, ancora, D. TROTTIER, *Coming to Terms with Social Media Monitoring*, cit., p. 531.

[24] Nello stesso senso, S. ATERNO, *L'acquisizione dei dati personali tra misure antiterrorismo e intromissioni nella* privacy, in *Arch. pen*., 2016, p. 165; S. ATERNO – F. CAJANI, *L'acquisizione dei dati di traffico*, in AA.VV., Cyber Forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, p. 318.

debba essere interpretato in termini di assenza di restrizioni o configurazioni di *privacy*. In caso contrario, l'informazione, come detto, ha natura "ristretta".

Con riferimento al criterio *sub* d), invece, uno dei principali problemi che sembra porsi riguarda la corretta interpretazione dell'espressione "misura di sicurezza". La maggior parte dei gestori di piattaforme *online* richiede all'utente un'iscrizione previa attraverso appositi moduli, la cui compilazione è necessaria per poter utilizzare i servizi di comunicazione e di *sharing*, nonché, talvolta, anche solo per poter semplicemente visualizzare le informazioni diffuse all'interno della "rete virtuale".

In tale contesto, la preventiva registrazione mediante l'utilizzo di credenziali specifiche (generalmente, profilo utente e *password*) potrebbe *prima facie* far propendere per la natura "non pubblica" delle informazioni contenute nei *social network*; esse, infatti, non sarebbero "a libero accesso", bensì fruibili soltanto da coloro che risultano iscritti alla piattaforma. A tale riguardo, del resto, il *Police Executive Research Forum* – la più importante organizzazione americana che riunisce i dirigenti delle forze dell'ordine statali e federali – definisce i *public domain data* come «informazioni accessibili tramite *Internet* per le quali non è necessaria una *password*, un indirizzo *e-mail* o altri identificatori al fine della loro visualizzazione, apprensione e successiva analisi»[25].

Un'esegesi di tal segno, tuttavia, parrebbe peccare di formalismo, finendo per restringere di molto il campo applicativo della categoria in esame[26].

L'assenza di una "misura di sicurezza", quale presupposto della natura "pubblica" del dato, è volta a evitare che siano qualificate come pubbliche tutte quelle informazioni ottenute in maniera occulta e fraudolenta da chi non ha la titolarità per accedervi, come nel caso – già ricordato – in cui un soggetto, sotto falso nome o utilizzando un *nickname*, induca l'utente a farsi "accettare" tra i propri "amici" o *followers*, al fine di carpire informazioni che lo stesso aveva scelto di mantenere "ristrette". Questa lettura pare trovare sostegno in un recente *report* prodotto dalla Commissione europea dedicato alle attività di *open source intelligence*[27]. Nella categoria dei *public available data*, infatti, vengono espressamente ricondotte tutte quelle notizie ricavate dai «*public media*», da «*internet*» e dalle «*professional and academic publications*»[28], cioè da fonti che, pur potendo richiedere una previa registrazione per il loro ottenimento (come nel caso di accesso a determinate riviste

---

Contra, E. DE BUSSER, *Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be USed Against You*, in *Groningen Journal of International Law*, 2014, p. 97.

[25] POLICE EXECUTIVE RESEARCH FORUM, *Social Media and Tactical Considerations For Law Enforcement*, 2013, p. 14 (trad. nostra).

[26] Sulla stessa linea interpretativa sembrano collocarsi pure J. ZARAGOZA TEJADA, *Ciberpatrullaje e investigación tecnológica en la red. Una aproximación a la inteligencia artificial desde el punto de vista de la investigación y represión de hechos ilícitos*, in *Cibercrimen III: inteligencia artificial, automatización, algoritmos y predicciones en el derecho penal y procesal penal*, coordinato da M. Kiefer, Buenos Aires, 2020, p. 214; M.J. HODGE, *The Fourth Amendament and Privacy Issues on the New Interent: Facebook.com and Myspace.com*, in *Southern Illinois University of Law Journal*, 2006, p. 108, per la quale «*the fact that the police need a password to sign on to MySpace, could [not] be argued to deem some expectation of private area*».

[27] Su tale concetto, v. *infra* par. 3.

[28] COMMISSIONE EUROPEA, *Open Source Intelligence*, 2 maggio 2022.

scientifiche, anche a pagamento[29]) devono, nondimeno, essere classificate come "pubblicamente accessibili".

Alla luce di quanto osservato, dunque, appare preferibile annoverare nella categoria delle *open source information* ricavabili dai *social network* tutti quei dati che, indipendentemente dal loro contenuto, sono liberamente accessibili, ovverosia "non chiusi" o ad accesso ristretto (*rectius*, limitato a determinate categorie di soggetti), ciò sia con riguardo a informazioni sensibili di carattere personale, sia in relazione a informazioni a carattere non personale.

3. Alle origini del cd. *cyberpatrolling*: sorveglianza di massa, controllo individualizzato e SOCMINT

Le operazioni investigative di raccolta e analisi di fonti liberamente accessibili (nei termini appena indicati) nascono e si sviluppano nell'ambito delle attività di *intelligence* governative[30] volte a garantire la sicurezza nazionale e la difesa dell'ordinamento costituito[31]. È in questo settore, infatti, che venne utilizzata per la prima volta la locuzione *open source intelligence* (OSINT) per alludere a quell'insieme di pratiche dirette a individuare, selezionare, estrapolare ed esaminare, in modo sistematico, "informazioni grezze" pubblicamente disponibili, senza la necessità di ricorrere a operazioni occulte o clandestine di acquisizione[32]. L'obiettivo perseguito dai Servizi segreti, in questo contesto, era (ed è tutt'ora) quello di raccogliere e trattare dati liberamente accessibili, al fine di produrre *report* informativi per i referenti istituzionali (Governo, Parlamento, etc.) atti a influire sui loro processi decisionali.

Prima dell'avvento della Rete, questo tipo di operazione era compiuta esclusivamente nel "mondo fisico", mediante la raccolta e lo studio di dati ricavati dalla stampa e dalle radio. L'*intelligence* sulle fonti aperte, in ogni caso, era considerata soltanto come una tra le numerose attività di spionaggio utilizzate dai Servizi[33], e i dati da essa ricavati costituivano

[29] L. REITANO, *Esplorare* Internet. *Manuale di investigazione digitale e* Open Source Intelligence, Bologna, 2014, p. 25.

[30] Ovverosia, quel «processo che inizia con la ricerca di informazioni della più diversa natura, prosegue con la relativa analisi e sfocia in un quadro di valutazioni volte alla comprensione e alla previsione di eventi futuri» (così, G. CONSO, *Sicurezza tra informazione, segreto e garanzie*, in *Per aspera ad Veritatem*, 1995, p. 27).

[31] La nascita dell'OSINT è comunemente fissata nel 1941, anno in cui il Presidente Roosevelt ordinò la realizzazione del *Foreign Broadcast Monitoring Service*, il cui obiettivo era quello di tradurre, trascrivere e analizzare programmi radiofonici di propaganda antistatunitense con il fine di tutelare la sicurezza nazionale. Di poco precedente, invece, il *BBC Monitoring*, una tecnologia sviluppata nel contesto britannico nel 1939 che consentiva di selezionare e tradurre informazioni ottenute dall'analisi di stampa e radio. Per approfondimenti, v. L. REITANO, *Esplorare* Internet, cit., p. 21 ss.; M. MARMO, Social media mining. *Estrarre e analizzare informazioni dai* social media, Milano, 2016, *passim*.

[32] Tra le definizioni più autorevoli di OSINT, può riproporsi quella fornita dal NATIONAL OPEN SOURCE ENTERPRISE, *Intellligence community directive number 301*, 2006: «*open source intelligence is produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement*». Per una panoramica sui contenuti e l'evoluzione della OSINT, cfr., *ex plurimis*, B. MILLER, *Open Source Intelligence (OSINT): An Oxymoron*, in *International Journal of Intelligence and Counter Intelligence*, 2018, p. 702 ss.; B.J. KOOPS – J. HOEPMAN – R. LEENES, *Open source Intelligence and Privacy by Design*, in *Computer Law and Security Review*, 2013, p. 676 ss.

[33] Nell'ambito dell'*Intelligence* possono distinguersi cinque tipologie di attività investigative: a) *Human Intelligence* (HUMINT), ovverosia l'ottenimento di informazioni da una rete di fonti umane (cd. informatori confidenziali); b) *Imagery Intelligence* (IMIT), cioè la raccolta di dati provenienti dallo studio delle immagini (satellite, aerei spia etc.); c) *Signal Intelligence* (SIGINT), ossia la raccolta automatizzata di dati grazie

una minima parte della totalità delle informazioni disponibili, specialmente se paragonati a quelli ottenuti da forme di *intelligence* relative alle cd. fonti protette o chiuse[34].

La proliferazione di *public available data* connessa alla diffusione di *Internet*, però, ha contribuito all'ascesa dell'attività di *open source* che, grazie ai numerosi contenuti disponibili nel *web*, è passata dall'essere considerata come una mera «*frosting on the cake*» alla «*large part of the cake itself*»[35], divenendo la tecnica principale di raccolta di dati nell'ambito delle attività di *intelligence* realizzate dai Servizi segreti[36].

Da quest'angolo di visuale, perciò, non v'è da stupirsi se oggigiorno simili operazioni sono compiute prevalentemente nei *social network* che, come si è sottolineato a più riprese, costituiscono la principale fonte di informazioni pubblicamente accessibili. È in tale contesto, pertanto, che si è sviluppata una peculiare tecnica di ricerca denominata *social network intelligence* (o *social media intelligence*). Quale *species* di attività *open source*, la SOCMINT consiste essenzialmente nella raccolta e nell'estrazione di notizie dalle differenti piattaforme digitali di comunicazione[37]. L'operare congiunto dei *big data* prodotti dalle interazioni degli utenti e delle potenzialità offerte dall'*intelligence* su fonti aperte ha dato vita a prospettive di ricerca del tutto nuove: «ciò che prima andava faticosamente cercato nelle pagine dei giornali, nell'ascolto di remote trasmissioni radio o tramite partecipazione diretta a eventi e riunioni […] viene oggi offerto e "portato in casa" dell'analista»[38] mediante una semplice ricerca automatizzata nella più grande (e qualitativamente significativa) banca dati del mondo.

3.1 Il *social network patrolling*: una nuova frontiera investigativa

Com'era prevedibile, le potenzialità offerte dalla SOCMINT sono state colte anche nel contesto della giustizia penale[39]. Preso atto del crescente utilizzo delle reti digitali per finalità

---

all'impiego di strumenti di captazione occulta di comunicazioni tra persone (cd. *Comunication Inteligence* – COMINT) o tra macchine (cd. *Electronics Intelligence* – ELINT); d) MASINT, ovvero l'apprensione di informazioni secondo schemi non classificati. Cfr., *amplius*, L. REITANO, *Esplorare* Internet, cit., p. 21.

[34] A. CORNELI, *Informazione e sicurezza. Il ruolo delle "fonti aperte"*, in *Rivista italiana di intelligence*, 2007, p. 25.

[35] J. GANNON, *The Strategic Use of Open Source Information*, in *Intelligence Community Persepctive*, 2014, p. 67.

[36] V., ancora, J. GANNON, *The Strategic Use of Open Source Information*, cit., p. 68, il quale sottolinea come «*open-source information now dominates the universe of the intelligence analyst*». Più nel dettaglio, A. HULNICK, *The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?*, in J. Johnson (a cura di), *The Oxford Handbook of National Security Intelligence*, Oxford, 2010, p. 230, mette in luce come le operazioni di *open source* occupino circa l'80% dell'intera attività di *intelligence*. Nello stesso senso si esprime D. CURTOTTI, *Procedimento penale e* intelligence *in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Proc. pen. gust.*, 2018, p. 446, nt. 38. In generale, sui benefici della OSINT nel contesto dell'attività di *intelligence*, v. i contributi pubblicati in C. HOBBS – M. MORAN - D. SALISBURY (a cura di), *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities*, Londra, 2014.

[37] L'espressione è stata coniata nel 2012 da S.D. OMAND – J. BARTLET – C. MILLER, *Introducing Social Media Intelligence (SOCMINT)*, in *Intelligence and National Security*, 2012, p. 801 ss.

[38] C. COMELLA, *Origine dei big data*, in *Rivista italiana di Intelligence*, 2017, p. 139. Non deve affatto stupire, perciò, se James Clapper, *ex* direttore dei Servizi segreti degli Stati Uniti, ha descritto i *social network* come le fonti principali per lo svolgimento di attività di *intelligence* («*huge for intelligence purposes*»).

[39] Cfr. F. SAMPSON, *Following the Breadcrumbs: Using Open Source Intelligence as Evidence in Criminal Proceedings*, in B. Akhgar – P.S. Bayler – F. Sampson (a cura di), *Open Source Intelligence Investigation. From Strategy to Implementation*, Cham, 2016, p. 295, il quale sottolinea come «*the provenance, collation, interpretation, analysis and deployment of open source intelligence (OSINT) is becoming a highly topical and*

illecite[40], è divenuta sempre più pressante l'esigenza di monitorare le attività *open space* realizzate dagli utenti. Un'operazione, quest'ultima, che appare non solo necessaria, ma anche doverosa, perlomeno qualora si acceda all'idea (qui condivisa) che gli strumenti di contrasto alla criminalità debbano operare tanto nel mondo fisico, quanto nell'universo digitale. In una "società iperconnessa" nella quale numerose attività di vita quotidiana sono ormai compiute *online*, l'ordinamento ha l'obbligo giuridico di garantire sicurezza e vigilanza pure nel contesto virtuale.

Solo di recente, però, gli studiosi (e, prima ancora, i pratici del diritto) hanno cominciato a interrogarsi sulla reale applicabilità e spendibilità processuale di metodologie investigative consistenti nel "rastrellamento" di informazioni pubblicamente disponibili nella Rete, tanto nella fase di *intelligence*, quanto in quella di prevenzione e repressione delle condotte illecite.

È in tali coordinate teoriche che la letteratura statunitense – nel contesto della *criminal open source intelligence* o *intelligence* criminale su fonti aperte[41] – ha coniato il termine *cyberpatrolling* per descrivere quell'insieme di attività di osservazione, monitoraggio, raccolta e analisi di informazioni pubblicamente disponibili, mediante il ricorso alle tecniche di *open source intelligence*[42]. Con specifico rifermento alle piattaforme digitali, il connubio tra le attività di "pattugliamento nei *social network*" e gli strumenti di SOCMINT ha dato vita a quella che appare definibile come una vera e propria nuova metodologia di indagine penale digitale: il *social network patrolling* o *social network monitoring*.

L'importanza assunta da questa tecnica è ben rappresentata dalle parole con le quali la Commissione europea ha reso noti gli esiti di uno studio condotto nell'ambito del progetto COMPOSITE (*Comparative police studies in the EU*) che, a sua volta, si inserisce nel solco dell'*EU's Seventh Framework Programme* (FP7) dedicato al tema della sicurezza: «*police patrolling social media. From the city's mean streets to Facebook, the police […] have expanded their beat from the streets outside our door to the virtual pathways of social media*»[43]. Il *report* di sintesi elaborato dalle istituzioni comunitarie (*Best Practice in Police Social Media Adaptation*) mette in evidenza in maniera chiara, sintetica, ma particolarmente efficace, i possibili impieghi dei *social network* nel contesto delle attività di *law enforcement*

---

relevant area of policing»; A. STANIFORTH, *Police Use of Open Source Intelligence: The Longer Arm of Law*, in B. Akhgar – P.S. Bayler – F. Sampson (a cura di), *Open Source Intelligence Investigation*, cit., p. 21 ss.; F. MASSA, Osint *e Cyber intelligence: tecniche di investigazione nella rete*, in *Sicurezza e giustizia*, 21 gennaio 2016.

[40] Cfr. Parte I, Cap. II, par. 3.

[41] Trattasi, più in particolare, di quell'attività orientata alla produzione di informazioni necessarie per fondare una decisione in materia di sicurezza pubblica, politica criminale e persecuzione penale. I destinatari del *report* di *intelligence* possono essere autorità amministrative, forze di polizia e l'autorità giudiziaria. Va considerato, peraltro, che oggigiorno l'*intelligence* criminale su fonti aperte rappresenta la forma di *intelligence* penale più importante dal punto di vista qualitativo e quantitativo (per dette considerazioni, v. L. MARZELL, *OSINT as a Part of the Strategic National Security Landscape*, in B. Akhgar – P.S. Bayerl – F. Sampson (a cura di), *Open Source Intelligence Investigation*, cit., p. 3).

[42] L'espressione, com'è evidente, denota numerose affinità con la locuzione *cyber intelligence* (alla quale si richiama), cioè l'operazione di ricerca, analisi e trattamento di dati raccolti da fonti diverse e in base a criteri predeterminati, al fine di estrarre informazioni impiegabili in vari contesti (es. *marketing*, giornalismo, etc.). Sul punto, v. G. COSTABILE, *Le indagini digitali*, in AA.VV., Cyber Forensics *e indagini digitali*, cit., p. 76.

[43] *https://cordis.europa.eu/article/id/35325-police-patrolling-social-media*.

e *crime investigation*. Tra questi, particolare attenzione è dedicata al tema dei «*social media as a source of criminal information*», ovvero all'impiego delle piattaforme digitali alla stregua di vere e proprie banche dati dalle quali attingere per la raccolta di informazioni processualmente rilevanti. In tale contesto, il documento citato sottolinea come uno dei principali strumenti di indagine nell'attuale società tecnologica sia rappresentato proprio dall'apprensione di dati *open source* contenuti nelle piattaforme di comunicazione: «*for investigations, the police can make use of open sources that include all information that is publicly available [on social network]*»[44].

Prima di esaminare nel dettaglio questa tecnica investigativa e i suoi riflessi sul piano *stricto sensu* probatorio, si rendono necessarie alcune precisazioni di carattere preliminare, volte a delimitare e meglio precisare l'oggetto della presente trattazione.

La prima, di tipo sistematico.

Non v'è dubbio che il monitoraggio dei *social network* possa essere annoverato tra le «attività *lato sensu* di "spionaggio"»[45] aventi natura tecnologica: trattasi, in effetti, di un'operazione inavvertita da chi la subisce e, al contempo, invasiva della sfera giuridica del bersaglio (indagato o terzo), il quale fornisce inconsapevolmente dati e informazioni all'autorità procedente. Quest'ultima circostanza, è opportuno sottolinearlo, non esclude affatto la possibilità di qualificare l'atto in questione come occulto e clandestino, posto che il soggetto, pur rinunciando in parte alla propria riservatezza nel momento in cui rende conoscibile a terzi informazioni originariamente riservate, non ha certamente la consapevolezza di essere sottoposto a un controllo esterno da parte dell'autorità statale. Ed è proprio per siffatta ragione che, richiamando la tradizionale classificazione proposta, ancora una volta, dalla letteratura americana[46] – ma, recepita anche dalla dottrina italiana[47] –, è possibile ricondurre il *social network monitoring* pure nell'alveo di quelle *new surveillance technologies* volte alla raccolta massiva di informazioni provenienti da fonti pubbliche o aperte al pubblico, successivamente analizzate con la finalità di individuare quella percentuale che potrebbe essere rilevante per le indagini (cd. *high volume collection*).

A livello naturalistico, poi, l'attività di monitoraggio dei *social network* può essere compiuta dall'autorità procedente mediante un profilo privato, riconducibile allo stesso agente di polizia, ovvero con il ricorso a un profilo *fake* creato *ad hoc*, utilizzando un *nickname* di fantasia (cd. *sock puppets*)[48]. A ben vedere, però, la distinzione, sul piano *stricto*

---

[44] *Best Practice in Police Social Media Adaptation*, 2012, p. 13-14, al sito *https://www.fit.fraunhofer.de/content/dam/fit/de/documents/COMPOSITE-social-media-best-practice.pdf*.

[45] C. CONTI, *Sicurezza e riservatezza*, in *Dir. pen. proc.*, 2019, p. 1573, la quale riconduce a questa macrocategoria anche l'acquisizione dei tabulati telefonici, le intercettazioni mediante *trojan* di Stato, le videoriprese e l'uso dei droni per finalità investigative.

[46] Il riferimento è a R. SIMMONS, *The Power and Pitfalls of Technology, Technology-Enhanaces Surveillance by Law Enforcement Officials*, in *NYU Annual Survey of American Law*, 2005, p. 712, il quale distingue, nel contesto delle *new surveillance technologie*, tra *hyper-intrusive search*, *virtual surveillance* e *hight volume collection*. Per un compiuto esame di tale classificazione, v. G. DI PAOLO, *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2008, p. 18-22.

[47] *In primis*, da G. DI PAOLO, *"Tecnologie del controllo" e prova* penale, cit., p. 18 ss.

[48] Un *sock puppet* è uno strumento che consente alle forze dell'ordine, nello svolgimento delle attività di *cyberpatrolling* (e non solo), di creare un'identità digitale falsa per infiltrarsi nei canali aperti di comunicazione.

sensu giuridico, appare irrilevante, poiché entrambe le attività, in assenza di una qualunque forma di interazione con il bersaglio, sono destinate a confluire nell'orbita della "perlustrazione" nei *social network*[49].

La seconda precisazione, invece, ha carattere terminologico.

Lo studio della (scarna) letteratura nazionale e internazionale in materia non consente, quantomeno allo stato attuale, di enucleare una nozione unica e condivisa di *cyberpatrolling* e di *social network monitoring*. Talvolta si ricorre a queste locuzioni per descrivere un insieme di tecniche finalizzate alla sola prevenzione dei reati, escludendo espressamente ogni riferimento ad attività connesse alla repressione delle condotte illecite (*post notitia criminis*)[50]; talaltra, invece, il termine viene impiegato in contrapposizione con l'espressione *web-patrolling*: nel primo caso, la vigilanza è realizzata dalle autorità di *law enforcement* avendo quale oggetto dati pubblici; nel secondo, invece, l'operazione viene compiuta dopo aver acquisito una notizia di reato, e richiede un intervento tecnico di intromissione nella sfera privata altrui. Ai fini della presenta analisi, la locuzione sarà utilizzata indistintamente con riguardo a tutte le fasi procedimentali (e pre-procedimentali), poiché, come si avrà modo di constatare, l'impiego di questa nuova tecnica investigativa pare estendersi a tutti i settori della giustizia penale (*intelligence*, prevenzione e repressione dei reati)[51].

Ciò che occorre sottolineare, casomai, è che si tratta, in ogni caso, di un'attività realizzata su informazioni *open access*. La precisazione risulta quantomai significativa, almeno sotto una duplice prospettiva.

In primo luogo, perché consente di mettere in luce la differenza concettuale tra il *cyberpatrolling* e le investigazioni digitali sotto copertura. Nel primo caso, l'osservazione e la successiva apprensione di informazioni avvengono nell'ambito di fonti aperte, cioè liberamente accessibili da chiunque. Al contrario, i *digital undercover operators* si muovono in canali di comunicazione chiusi, cioè in luoghi del cyberspazio nei quali l'accesso è subordinato alla titolarità di una precisa qualifica e, soprattutto, finalizzato all'interazione con un determinato bersaglio per l'ottenimento di informazioni utili a fini investigativi[52].

---

[49] Pare avallare indirettamente questa conclusione anche P. TROISI, *Le investigazioni digitali sotto copertura*, Bari, 2022, p. 89, 180.

[50] È questa, ad esempio, l'impostazione adottata da una parte della dottrina spagnola. Alcuni A., infatti, distinguono, nell'ambito della categoria del «*rastreos informáticos*», l'attività di «*ciber-patrullaje*», finalizzata «*a la vigilancia, prevenciòn y evitaciòn de ilìcitos cuya evidencia conste en la red*», da quella di «*análisis de fuentes abiertas*», diretta «*a la bùsqueda de informaciones que contribuyan al esclarecimiento de los hechos delictivos ya cometidos y que son objecto del interès del proceso penal*» (in questi termini, G. DELGADO MARTÍN, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Madrid, 2018, p. 107). Nello stesso senso, altra parte della dottrina suole operare una differenziazione tra l'attività di *ciberpatrullaje* e quella di *ciberinvestigación* (v. P. MARTIN RIOS, *Digital forensics and criminal process in Spain: evidence gathering in a changing context*, Cizur Menor, 2022, p. 167; M. TAVORA SERRA, *Ciberpatrullaje en el medio virtual. Delimitando conceptos*, in *Ius et Scientia*, 2023, p. 89).

[51] Come sottolinea pure F. BUENO DE MATA, *Investigación y prueba de delitos de odio en Redes Sociales*, cit., p. 168, il *ciberpatrullaje* o *tecnovigilancia* non deve essere associato esclusivamente a questioni relative alla prevenzione dei delitti, giacché esso ben può essere impiegato anche «*para averiguar delitos en espacios abiertos en los que ya se han cometido*».

[52] Rilevano tale distinzione, ad es., anche P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 74; M. TEMPERINI, *Delitos informàticos y cibercimen: tècnicas y tendencias de investigaciòn penal y su afectaciòn a los derechos constitucinales*, in D. Dupuy – J. Corvalàn (a cura di), *Cibercrimen III*, Montevideo, 2020, p. 249.

In secondo luogo, la circostanza che l'attività di *social network monitoring* abbia ad oggetto informazioni immesse volontariamente in Rete dagli utenti consente di distinguerla dalle operazioni di cd. *police fishing*, realizzate dagli "agenti digitali attrezzati per l'inganno"[53]. Rinviando la trattazione di questa specifica (e controversa) tematica ai capitoli successivi, è opportuno fin d'ora sottolineare come l'attività investigativa che sfrutta l'utilizzo di profili falsi – o, comunque, l'impiego di strumenti atti a dissimulare la vera identità dell'agente di polizia al fine di carpire informazioni altrimenti inaccessibili (poiché protette da impostazioni di *privacy* che ne limitano la conoscibilità a taluni soggetti) – non può essere ricompresa nell'ambito del *cyberpatrolling*. Il concetto di dato digitale *open access*, lo si è visto, evoca solamente quelle informazioni pubblicamente accessibili da chiunque; tali non sono, invece, quelle rispetto alle quali l'utente ha imposto una certa ristrettezza[54].

La terza precisazione ha carattere *stricto sensu* normativo.

A differenza di quanto previsto in altri ordinamenti[55], in Italia non vi è, né a livello di fonte primaria, né a livello regolamentare, una disciplina specifica e dettagliata di simili attività. Neppure l'attuale quadro normativo europeo, peraltro, contempla espressamente l'attività di SOCMINT tra le nuove tecniche investigative a contenuto tecnologico. Ciò, come si avrà modo di osservare, rischia di generare frizioni, innanzitutto, con il principio di legalità processuale che, nel contesto delle investigazioni digitali (più che in altri[56]), è oggetto di interpretazioni che ne mortificano la reale portata garantista[57]; il timore, dunque, è di trovarsi nel mezzo di un «"*far-west* tecnologico", in cui il diritto soccombe alla tecnologia»[58].

Peraltro, pare solo il caso di osservare come la mancanza di una regolamentazione delle attività investigative condotte nei *social network* – e, in particolare, quella di *cyberpatrolling* – si pone in contrasto con le raccomandazioni di matrice comunitaria che, nel ricordato

---

[53] Cfr. *supra*, par. 1.

[54] La questione verrà trattata più approfonditamente nel prosieguo dello studio. Ciò nondimeno, è doveroso dare conto fin da ora del fatto che la tematica risulta assai controversa. L'esegesi proposta nel testo, in effetti, è avversata da quei (pochi) autori italiani che, affrontando incidentalmente il tema *de quo*, hanno sostenuto che l'attività di polizia diretta ad acquisire con l'inganno dati e informazioni *online* rientri a pieno titolo nelle operazioni di *open source intelligence*. In questa ipotesi – si sostiene –, l'utente ha liberamente e volontariamente accettato di entrare in contatto con il "falso poliziotto": nessuna aspettativa di *privacy*, perciò, può essere legittimamente invocata (in questo senso, v., ad es., A. APRUZZESE, *La recente normativa in tema di contrasto del terrorismo e del proselitismo tramite* web. *Nuovi modelli di normative di prevenzione e nuovi schemi di indagini proattive*, in AA.VV., *La giustizia penale preventiva. Ricordando Giovanni Conso*, Milano, 2016, p. 234).

[55] B.J. KOOPS, *Police Investigations in Internet Open Source: Procedural-Law Issues*, in *Computer Law & Security Review*, 2013, p. 658.

[56] Il lento, ma pervasivo, percorso di "destrutturazione" del principio di legalità nel processo penale contemporaneo è stato messo in luce da numerosi autori. Cfr., per tutti, P. NUVOLONE, *Legalità penale, legalità processuale e recenti riforme*, in *Riv. it. dir. proc. pen.*, 1984, p. 3 ss.; M. NOBILI, *Principio di legalità e processo penale*, in *Riv. it. dir. proc. pen*., 1995, p. 648; T. PADOVANI, *Il crepuscolo della legalità nel processo penale. Riflessioni antistoriche sulle dimensioni processuali della legalità penale*, in *Ind. pen*., 1999, p. 527 ss.

[57] Ci si riferisce alla nota tendenza giurisprudenziale di ricondurre una serie di attività investigative non disciplinate dalla legge (come, ad esempio, il pedinamento GPS, il riconoscimento fotografico o le perquisizioni *online* tramite *trojan*) nella copertura assicurata dall'art. 189 c.p.p.

[58] M. PANZAVOLTA, *Intercettazioni e spazio di libertà, sicurezza e giustizia*, in F. Ruggieri – L. Picotti (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 69.

documento pubblicato all'esito del progetto *Comparative police studies in the EU*, richiedono agli Stati membri di adottare discipline *ad hoc* in tema di indagini penali svolte in ambiente virtuale («*investigations in social media require a legal framework*»), sottolineando, a tal proposito, come «*existing legal frameworks need to be transposed to social media*»[59].

Infine, la quarta considerazione è volta a mettere in luce le potenzialità sottese al *cyberpatrolling*.

La tecnica investigativa che si va esaminando non si limita alla raccolta di singoli dati pubblicamente disponibili, quale è l'estrazione delle informazioni di contatto (nome, cognome, *nickname*, indirizzo di posta elettronica, numero di telefono, data di nascita, attività lavorativa, etc.), di immagini, commenti o dichiarazioni rese nei *social network*. Tutt'altro. Grazie all'impiego di *software*[60] che sfruttano l'intelligenza artificiale è possibile ottenere una panoramica incredibilmente dettagliata delle abitudini di vita di una certa collettività o di un singolo individuo. Il conteggio del numero di *post*, la loro frequenza di pubblicazione, i siti visitati, l'analisi delle interazioni, la partecipazione a "gruppi virtuali" o a eventi pubblici, i rapporti familiari, gli *hobbies*, gli spostamenti, la geolocalizzazione, nonché l'esame dei metadati prodotti da ogni singola attività digitale[61], oltre a lasciare un'impronta indelebile nell'universo virtuale, sono un chiaro esempio di applicazione della cd. *Mosaic Theory*. Il riferimento va a quell'idea – sistematizzata da autorevole dottrina – in base alla quale la raccolta e l'aggregazione massiva di dati prodotti da attività prolungate di vigilanza digitale è in grado di comporre il "mosaico" delle abitudini quotidiane e delle relazioni sociali dei soggetti sottoposti a controllo, consentendo alle autorità di ottenere informazioni fondamentali per il buon esito dell'attività investigativa[62].

Per tale ragione, dunque, non sembra azzardato affermare che una ricerca di informazioni sui *social network* in uso a un determinato soggetto «spesso rivela molto di più di una semplice perquisizione presso la sua residenza»[63]. In tale prospettiva, ben si comprende

---

[59] Per le due ultime citazioni, v. le *Best Practice in Police Social Media Adaptation*, 2012, cit. p. 14.

[60] Per una rassegna, v. G. COSTABILE, *Le indagini digitali*, cit., p. 86 s.

[61] Per una "carrellata" delle diverse informazioni che possono essere estratte mediante l'impiego della tecnica SOCMINT, v. F. BUENO DE MATA, *Investigación y prueba de delitos de odio en Redes Sociales*, cit., p. 98-100. Emblematica, in tal senso, è l'applicazione *Tinfoleak*. Il *software* consente di automatizzare la fase di ricerca, estrazione e valutazione delle informazioni, rendendo possibile l'analisi del contenuto di un *tweet*, come le parole utilizzare, gli *hashtag* e il tipo di contenuto multimediale. Per una descrizione dettagliata dei metadati che possono ricavarsi da un *tweet*, cfr. *https://blog.0day.rocks/you-will-be-surprised-by-what-your-tweets-may-reveal-about-you-and-your-habits-3bc907688bc8*, nonché, per i metadati estraibili da *Telegram*, M. GIARRUZZO – N. MARINI, *Attività illecite su* Telegram: *la* social media intelligence *a supporto delle indagini*, in *Sicurezza e giustizia*, 21 luglio 2020.

[62] O.S. KERR, *The Mosaic Theory of the Fouth Amendament*, in *Michigan Law Review*, 2012, p. 311 ss. La "teoria del mosaico", in realtà, è stata affermata per la prima volta nelle *concurring opinions* dei giudici Sotomayor e Alito rese nel caso *Stati Uniti c. Jones*, 565. 400 (2012), allorquando si è sostenuto che l'apprensione in maniera aggregata e continuativa dei *public movements* di una persona, anche se individualmente non protetti dal IV emendamento, «*reveals types of information not revealed by short-term surveillance*», cosicché deve ritenersi sussistente una ragionevole aspettativa di *privacy* in capo al soggetto controllato. Sul punto, cfr. D. GRAY – D.K. CITRON, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendament Privacy*, in *North Carolina Journal of Law and Technology*, 2013, p. 381 ss.

[63] B. MUND, *Social Media Searches and the Resonable Expectation of Privacy*, in *Yale Journal of Law and Technology*, 2017, p. 260 (trad. nostra).

come il *cyberpatrolling* non si esaurisca in una semplice operazione di osservazione e trattamento di informazioni pubbliche, ma possa potenzialmente consentire un monitoraggio continuativo delle attività compiute dagli utenti (o dal singolo cibernauta) – nonché di quelle realizzate nel passato –, all'esito del quale è possibile ricostruire *ex post* le loro idee, opinioni e interessi[64].

3.2 *Cyberpatrolling* e società del controllo: lo Stato vigilante nell'era della cd. *coveillance*

La circostanza da ultimo evidenziata – ovverosia che le forme più recenti di pattugliamento digitale nei *social network* possono provocare un'ingerenza stabile e duratura nella sfera di libertà degli "abitanti del *web*" – rischia di trasformare dette attività in forme occulte di «sorveglianza digitale»[65]. La sorveglianza, come noto, è un fenomeno sociale, culturale e politico che interessa da sempre la collettività, gli individui e le entità titolari del potere. Se le prime forme embrionali di controllo sociale sono rinvenibili addirittura nell'Impero Romano[66], è solo con la nascita delle moderne democrazie liberali che si è assistito al definitivo passaggio da una sorveglianza positivamente finalizzata alla gestione ad ampio raggio dell'apparato statale-amministrativo[67], a una *new surveillance* di tipo occulto (o sorveglianza contemporanea), il cui reale obiettivo – a dispetto di un'ostentata esigenza di garantire maggiore sicurezza – è spesso quello di realizzare uno *screening* della cittadinanza, specialmente per finalità commerciali e, più in generale, assicurare un controllo sull'opinione sociale.

Questo mutamento di prospettiva è strettamente legato all'avvento delle nuove forme di tecnologia dell'informazione, allo sviluppo della cd. *Internet of Things* e all'impiego sempre più diffuso dei *social network*, sistemi nei quali le persone e gli oggetti di vita quotidiana sono in grado di produrre una vasta gamma di risorse informative[68]. Come si è avuto modo

---

[64] Sui rischi connessi all'impiego di attività investigative volte a una vera e propria «mappatura dei *social network*», v., esplicitamente, Corte edu, 25 maggio 2021, *Big Brother Watch e altri c. Regno Unito*, par. 342 (trad. nostra).

[65] Sul concetto di sorveglianza digitale, imprescindibili gli studi condotti da David Lyon, trai quali si ricorda, per tutti, D. LYON, *L'occhio elettronico.* Privacy *e filosofia della sorveglianza*, Milano, 1997.

[66] Il riferimento è al cd. censimento, cioè quello strumento che consentiva di ottenere un elenco comprensivo dei beni e degli averi di ogni cittadino.

[67] Perlomeno in un primo momento, infatti, il termine "sorveglianza" non era affatto circondato da un'aura negativa. Tutt'altro. Con la finalità di dotarsi di un apparato organizzativo efficiente ed efficace, gli Stati moderni del XIX secolo hanno introdotto strumenti per la raccolta e il trattamento di informazioni riguardati i singoli cittadini. In tal senso, la necessità di garantire il principio di uguaglianza (tanto in senso formale, quanto sostanziale), postulava che lo Stato fosse nella piena e legittima disponibilità di informazioni identificate su base individuale: per stabilire chi avesse diritto di godere di determinate prestazioni o sevizi pubblici, ad esempio, l'ordinamento necessitava di conoscere la titolarità dei beni dei singoli cittadini. In questa prospettiva, dunque, la sorveglianza costituiva un'attività palese, nonché il presupposto logico-necessario per poter gestire al meglio l'apparato burocratico statale (per approfondimenti, v. D. LYON, *L'occhio elettronico*, cit., p. 52; ma, già, S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, 1973 (Ristampa anastatica a cura di G. Alpa), Napoli, 2018, p. 29 s.).

[68] G. DI PAOLO, *"Tecnologie del controllo" e prova* penale, cit., p. 17, la quale sottolinea come «una gran parte delle informazioni relative agli aspetti più intimi della vita delle persone vengono raccolte proprio in conseguenza dell'uso che esse fanno, tanto in ambiti privati che pubblici, delle stesse tecnologie». Nello stesso senso, di recente, F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Milano, 2020, p. 4; e, con specifico riguardo proprio alle nuove piattaforme di comunicazione digitale, v. D. LOSAVIO

di sottolineare a più riprese, la tendenza, sempre più diffusa, degli internauti a condividere nel *web* tutti i momenti della propria vita quotidiana[69] ha contribuito a generare, nel contesto della cd. «*coveillance*»[70] (sorveglianza inversa), una gigantesca banca dati pubblicamente accessibile, delineando «un sistema di sorveglianza capillare che noi stessi, più o meno consapevolmente, alimentiamo, per l'incontenibile desiderio di condividere tutto ciò che ci circonda»[71]. In questi termini, la sorveglianza altro non è che l'altra faccia della medaglia rappresentata dalla libertà di opinione nel contesto digitale. Lo *sharing* di un'immagine con annessa geolocalizzazione (cd. *geo-tagging*) o il semplice *like* apposto a un commento su *Twitter* sono diventati un dato prezioso per formulare statistiche e controllare i movimenti di ogni singolo utente (*social network profiling*).

Dinnanzi a un simile scenario, lo studioso del rito penale non può rimanere indifferente.

Sennonché, deve condividersi l'affermazione di quegli attenti commentatori che, in una prospettiva più generale, hanno sottolineato come risulti «ancora deficitario l'impegno profuso dalla dottrina nell'indagare i risvolti connessi all'impiego delle nuove tecnologie di controllo occulto nella sede del processo»[72], specialmente – dovrebbe aggiungersi – in relazione ad attività intrusive che possono sfociare in forme di controllo costante e continuativo (*dataveillance*).

E proprio l'attività di *social network patrolling*, versione aggiornata dello Stato vigilante e della Società del controllo[73], sembra collocarsi in questa direzione, spingendosi fino a provocare un mutamento strutturale della fisionomia investigativa. La vigilanza mediante SOCMINT, infatti, è in grado di realizzare tanto una sorveglianza di massa (o non targettizzata), quanto una sorveglianza individualizzata. Con la prima espressione, com'è noto, si allude a quell'insieme di attività *untargeted* volte a raccogliere informazioni su un numero non predefinito di soggetti, nel contesto delle indagini penali o prima del loro

– M.M. LOSAVIO, *Prosecution and Social Media*, in C.D. Marcum – G.E. Higgins (a cura di), *Social Networking as a Criminal Enterprise*, Boca Raton, 2014, p. 201.

[69] Il fenomeno è stato icasticamente definito come «vetrinizzazione sociale» da V. CODELUPPI, *La vetrinizzazione sociale*, Torino, 2007.

[70] Il concetto, sistematizzato per la prima volta da S. MANN – J. NOLAN – B. WELLMAN, *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, in *Surveillance & Society*, 2003, p. 331 ss., è utilizzato nel contesto dei *social network* per descrivere la possibilità costante e biunivoca di osservare e di essere osservati.

[71] Queste sono le parole utilizzate dall'*ex* Garante della *privacy* Antonello Soro (*https://www.garanteprivacy.it/home/docweb/-/docweb-display/print/4612330*). Sembra essersi al cospetto, perciò, di una vera e propria forma di sorveglianza contemporanea (così come definita da D. TROTTIER, *Social Media as Surveillance: Rethinking Visibility in a Converging World*, Londra, 2012, p. 4), alimentata dal fenomeno della cd. *extimacy*, locuzione coniata in antitesi con il termine *intimacy* per descrivere l'atto di rendere pubblica la propria vita privata attraverso la Rete (cfr. L. TELLO-DÍAZ, *Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook*, in *Revista Cientifica de Comunicaciòn y Educaciòn*, 2013, p. 205 ss.; e, per le ripercussioni sul versante penalprocessuale, L. BACHMAIER WINTER, *Criminal Investigation and Right of Privacy: the Case-law of the European Court of Human Rights and its Limits*, in *Lex ET Scientia International Journal*, 2009, 2, p. 12 ss.).

[72] F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., p. 7 s. In precedenza, aveva colto questo aspetto D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Arch. pen*., 2016, p. 44.

[73] Anche secondo A. NIETO MARTIN – M. MAROTO, *Redes sociales en internet*, cit., p. 3, «*la utilizaciòn de facebook y el resto de redes sociales como forma de preneciòn e investigaciòn es una manifestaciòn màas del Estado vigilante y de la sociedad de control*».

formale inizio (cd. monitoraggio passivo o generico). La vigilanza mirata, invece, consiste in un'operazione di *screening* di un determinato bersaglio previamente individuato, con la finalità di acquisire dati in grado di supportare l'attività investigativa (cd. monitoraggio attivo o specifico).

4. Il campo d'azione del "pattugliamento virtuale": *intelligence*, prevenzione e repressione criminale

Come già sottolineato, l'espletamento del *social media monitoring* in ambito penale può astrattamente realizzarsi in tre differenti momenti: fase di *intelligence* (*i*), fase di prevenzione amministrativa (*ii*) e fase di repressione (*iii*).

È evidente come la diversa collocazione temporale e il differente ambito di applicazione soggettiva abbiano un riflesso immediato sul tipo e sul livello di tutele che l'ordinamento è chiamato ad approntare. Laddove tali operazioni vengano realizzate in maniera indiscriminata e generalizzata in una fase antecedente alla commissione del fatto di reato, si corre il rischio di giustificare forme di controllo totale e totalizzante sulla popolazione, cioè ipotesi occulte di *massive surveillance* destinate a sollevare problemi di compatibilità con quei principi generali posti a fondamento dello Stato di diritto di derivazione liberare che si pone come obiettivo la tutela delle libertà inviolabili dei cittadini. Viceversa, qualora l'attività sia soggettivamente orientata alla raccolta di informazioni relative a uno specifico bersaglio, occorrerà valutare se, in quali casi e con quali limiti l'ordinamento possa legittimamente apprenderle.

Si tratta, però, di interventi ermeneutici tutt'altro che agevoli da portare a compimento, dal momento che «le fasi idealmente consecutive [dell'*intelligence*] della prevenzione e della repressione si sono agglutinate»[74] a tal punto da rendere complessa l'individuazione di una netta linea di confine.

Con riferimento al primo binomio (*intelligence*-prevenzione), la distinzione a livello teorico è, tutto sommato, abbastanza agevole: alla luce di un criterio funzionale-finalistico, la prima è volta all'acquisizione di materiale informativo utile per la tutela della sicurezza dello Stato e delle sue istituzioni democratiche; l'attività di prevenzione, al contrario, ha quale unico scopo «il mantenimento dell'ordine pubblico in ciascun luogo e ciascuna parte dell'amministrazione generale; e tende principalmente a prevenire i reati»[75].

In relazione al secondo binomio (prevenzione-repressione), la dottrina più autorevole ha da tempo messo in evidenza come la distinzione debba essere rintracciata nell'antitesi tra "ricerca dei reati e ricerca di un reato"[76]: mentre l'attività della polizia di prevenzione è

[74] D. NEGRI, *La regressione della procedura penale ad arnese poliziesco*, cit., p. 45.

[75] P. TONINI, *Polizia giudiziaria e magistratura. Profili storici e sistematici*, Milano, 1979, p. 60. Per di più, mentre il lavoro dei Servizi Segreti «rappresenta l'effettività dello Stato puro, che non sente il bisogno di rappresentarsi sulla scena; è l'anti-messa in scena», il procedimento penale, al contrario, è forma pura, una forma necessariamente pubblica atta a garantire il controllo della collettività sul corretto esercizio della funzione di *ius dicere* (A. GARAPON, *Lo Stato minimo. Il neoliberalismo e la giustizia*, Milano, 2012, p. 104).

[76] In questi termini, richiamando una corrente interpretativa sviluppatasi nella dottrina francese agli inizi degli anni '70 del secolo scorso, che l'A. ritiene di condividere, P. TONINI, *Polizia giudiziaria e magistratura*, cit., p. 261.

diretta, per l'appunto, a «prevenire i danni sociali», la polizia giudiziaria ha lo scopo di «reprimere le violazioni di diritto già avvenute»[77].

Sennonché, queste distinzioni concettuali sembrano destinate a rimanere, in larga parte, *in the book.*

Lo sviluppo di tecnologie sempre più sofisticate, l'affermarsi di una criminalità quantitativamente e qualitativamente più efferata rispetto al passato[78] e la necessità di governare (o, quantomeno, tentare di governare) i nuovi e complessi fenomeni che caratterizzano la "società del rischio" hanno accelerato il processo di affermazione di un vero e proprio "Stato di prevenzione". In tale contesto, l'*intelligence*, come un fiume in piena, ha rotto gli argini invadendo il terreno della prevenzione; a sua volta, la prevenzione è riuscita a intaccare il "giardino sacro" dell'accertamento processuale mediante la configurazione di una nuova tipologia di attività – la cd. indagine proattiva[79] –, provocando, in un colpo solo, la definitiva caduta del muro che separava il mondo dell'*intelligence*, l'universo della prevenzione e la sfera giurisdizionale. Insomma, il cortocircuito è evidente[80] e di esso occorre prendere atto, con una sana dose di realismo[81].

Numerosi sono i profili problematici che si affacciano all'orizzonte.

In primo luogo, la «regressione della procedura penale ad arnese poliziesco»[82] e la distinzione, sempre più sfumata, tra polizia giudiziaria e polizia di sicurezza delineano un quadro nel quale le forze amministrative entrano nel circuito giudiziario e, parallelamente, le autorità giudiziarie «operano direttamente sul terreno della politica criminale che dovrebbe essere riservato [invece] all'autorità di pubblica sicurezza», imponendo di interrogarsi su «una delicata questione di equilibrio fra potere giudiziario e potere governativo»[83]. Senza considerare che, così facendo, si finisce per legittimare

---

[77] Così, per le due ultime citazioni, SANTI ROMANO, *Principii di diritto amministrativo italiano*, Milano, 1912, p. 245.

[78] Si vedano, in proposito, le penetranti (e convincenti) affermazioni di F. MANTOVANI, *Insicurezza e controllo della criminalità*, in *Riv. it. dir. proc. pen*., 2010, p. 1003 s., laddove sottolinea che «il diffuso senso collettivo di insicurezza non è il mero prodotto dell'amplificazione mediatica della criminalità, come talora viene sbrigativamente affermato anche nel mondo penalistico e criminologico. Bensì è un dato fondato sul duplice fenomeno: 1) dell'aumento quantitativo della criminalità, specie della "criminalità diffusa" […] che è quella che incide più negativamente sulla qualità della nostra concreta vita quotidiana […]; 2) del peggioramento qualitativo della criminalità, sempre più immotivatamente e sproporzionalmente violenta, crudele, sanguinaria, spregiudicata, irridente, precoce e minorile. Ed anche importata».

[79] Di una «contaminazione poliziesca del procedimento penale» ha parlato P.P. PAULESU, *La presunzione di non colpevolezza dell'imputato*, Torino, 2009, p. 113.

[80] Come ha messo in luce M. GIALUZ, *Banche dati europee e procedimento penale italiano*, in F. Peroni – M. Gialuz (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, p. 254, «parallelamente a quella tra attività di *intelligence* e attività di indagine penale, si è andata affievolendo la linea di separazione tra ispezione amministrativa e indagine penale».

[81] In proposito, osserva F. VIGANÒ, *Terrorismo, guerra e sistema penale*, in *Riv. it. dir. proc. pen.*, 2006, p. 694, che lo scienziato del diritto penale deve prendere atto «dell'inevitabilità di uno spostamento di accento, da parte del sistema penale nel suo complesso, dal paradigma della repressione di un fatto già commesso a quello della prevenzione di fatti non ancora commessi, in nome di una più efficace tutela della sicurezza collettiva».

[82] Richiamando la felice espressione di D. NEGRI, *La regressione della procedura penale ad arnese poliziesco*, cit., p. 44. Cfr. pure R.E. KOSTORIS, *Processo penale, delitto politico e «diritto penale del nemico»*, in *Riv. dir. proc.*, 2007, p. 4.

[83] Così, per le due ultime citazioni, R. ORLANDI, *Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali*, in AA.VV., *La giustizia penale preventiva*, cit., p. 16.

inconsapevolmente un modello di accertamento processuale della responsabilità penale alimentato con dati di origine esterna e occulta, rispetto ai quali un eventuale contraddittorio postumo appare, in talune circostanze, perlopiù inconsistente. In secondo luogo, va notato che l'assottigliarsi della linea di demarcazione tra fase di *intelligence*, universo preventivo e momento procedimentale – nell'ottica di un ripensamento in termini preventivi del complessivo sistema di giustizia penale – sembra aver legittimato il «rafforzamento del ruolo e dei poteri della polizia giudiziaria, nell'ambito di una più generale valorizzazione della fase investigativa, quando non di quella pre-investigativa [e di *intelligence*]»[84].

Il fenomeno appena descritto può essere osservato da una duplice prospettiva.

Esemplificativo, sotto un primo profilo, è il contenuto precettivo dell'art. 23, comma 1, l. 124/2007[85], ove si stabilisce che il personale in organico presso i Servizi segreti non riveste la qualifica di ufficiale o di agente di polizia giudiziaria né, tendenzialmente, quella di ufficiale o di agente di pubblica sicurezza. La preclusione risponde all'esigenza di riaffermare con estrema nettezza la distinzione funzionale tra i vari momenti investigativi e, specialmente, di garantire effettività al disposto dell'art. 109 Cost., evitando così che gli appartenenti ai Servizi di *intelligence* siano sottoposti alle direttive dell'autorità giudiziaria che, com'è intuibile, finirebbero per limitare quella naturale libertà nell'agire propria di chi è chiamato a difendere la sicurezza nazionale di un Paese.

La conseguenza di tale assetto sul versante processuale è estremamente significativa: gli agenti dei Servizi non sono tenuti a osservare le norme dettate dal codice di rito in relazione allo svolgimento delle indagini preliminari. Ciò, però, non significa affatto che essi non possano svolgere quelle attività che il codice di procedura penale riserva alla polizia giudiziaria[86]. Anzi, gli appartenenti all'*intelligence* debbono ritenersi legittimati a realizzare operazioni aventi un contenuto simile a quelle attribuite alla polizia giudiziaria[87]; così facendo, però, vi è il rischio che si vada legittimando l'ingresso nel procedimento penale di informazioni formate secondo crismi e regole estranee a quelle fissate nel codice.

Sotto un secondo profilo, va preso atto del recente incremento, nel contesto della polizia amministrativa e della polizia giudiziaria, di attività *lato sensu* investigative riconducibili alla categoria dell'*intelligence*[88], cioè volte alla raccolta e al trattamento massivo di dati e informazioni[89]. Il *cyberpatrolling* preventivo e repressivo, a ben considerare, costituisce la più evidente manifestazione di questa tendenza.

---

[84] S. LORUSSO, *Sicurezza pubblica e diritto emergenziale: fascino e insidie dei rimedi processuali*, in *Dir. pen. proc*., 2010, p. 274.

[85] L. 3 agosto 2007, n. 124 concernente il Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto.

[86] La tesi è stata sostenuta da C. COCCO, *I servizi di informazione e sicurezza nell'ordinamento italiano*, Padova, 1980, p. 61.

[87] Per questa opinione, v. M.L. DI BITONTO, *Raccolta di informazioni e attività di* intelligence, in R.E. Kostoris – R. Orlandi (a cura di), *Contrasto al terrorismo interno e internazionale*, Torino, 2006, p. 260.

[88] W. NOCERINO, *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, Milano, 2018, p. 218, nt. 148.

[89] Come ricorda R. ORLANDI, *Attività di* intelligence *e diritto penale della prevenzione*, in G. Illuminati (a cura di), *Nuovi profili del segreto di Stato e dell'attività di* intelligence, Torino, 2010, p. 236, «la raccolta ed elaborazione di dati sensibili e le schedature di determinate persone pedinate e osservate a distanza […] costituiscono, si può dire, il pane quotidiano di un servizio di sicurezza».

5. Servizi segreti e vigilanza continuativa: alla ricerca di un ragionevole equilibrio

A seguito dei tragici eventi di New York del 2001, gli ordinamenti nazionali di tutto il mondo hanno cominciato a implementare, in maniera assai più significativa rispetto al recente passato, sistemi di osservazione occulta e continuativa della collettività a opera delle forze di sicurezza nazionale (Servizi segreti)[90]. Queste attività di sorveglianza *untargeted*, com'è noto, sono state giustificate dalla necessità di neutralizzare il pericolo di futuri eventi lesivi o attentati alla sicurezza nazionale.

Nella condivisibile convinzione che la tutela della *tranquillitas* collettiva costituisca un valore «super primario […] imprescindibilmente legato alla vita, all'incolumità fisica, al benessere dell'uomo e alla qualità della sua esistenza, nonché alla dignità della persona»[91], i cittadini sono stati disposti a cedere quote della loro libertà in cambio della promessa di maggiore sicurezza[92]. E, in effetti, se dalla minaccia terroristica (e mafiosa) può derivare l'epilogo dello Stato democratico, appare più che legittimo, in ossequio a un principio di "autoconservazione statale", che l'ordinamento Costituito reagisca mediante la previsione di strumenti in grado di rispondere efficacemente alla minaccia in corso[93].

Sul versante penalistico, la lotta a fenomeni di terrorismo ed eversione dell'ordinamento democratico ha inciso non solo sul piano del diritto sostanziale (producendo sovente un arretramento della soglia di punibilità quale conseguenza di un nuovo «diritto penale al limite»[94]), ma, altresì, sul versante processuale. L'idea di fondo, a quest'ultimo proposito, è che il contrasto a tali fenomeni passi anzitutto dalla messa in opera di attività di prevenzione efficienti ed efficaci, mediante lo sviluppo di strumenti di indagine in grado, per l'appunto, di prevenire e "predire" il possibile realizzarsi di simili accadimenti grazie a un controllo diffuso e generalizzato di informazioni ritenute utili per la difesa della sicurezza nazionale[95].

---

[90] R. ORLANDI, *Sicurezza e diritto penale. Dialogo di un processualista italiano con la scuola di Francoforte*, in M. Donini – M. Pavarini (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, p. 95.

[91] G. CERRINA FERONI – G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi Costituzionali*, 2008, 1, p. 31. Sul valore riconosciuto alla sicurezza nell'attuale contesto sociale e giuridico, cfr. Parte II, Cap. I, par. 1.

[92] In questi termini, M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e* privacy, in *Federalismi.it*, 30 novembre 2016, p. 3. Anche la Corte costituzionale ha riconosciuto che «la scurezza si ha quando il cittadino può svolgere la propria lecita attività senza essere minacciato da offese alla propria personalità fisica e morale» (Corte cost., 23 giugno 1956, n. 2).

[93] Ciò, tuttavia, ha sovente portato il legislatore a adottare nel corso degli anni scelte di politica processuale improntate al "canone di emergenza", cioè all'idea per cui l'eccezionalità e la gravità della situazione giustifichi *tout court* una deroga ai principi fondamentali e imponga, contestualmente, un progressivo rafforzamento delle finalità preventive. Sul punto, cfr., *amplius*, G. RICCIO, *Politica penale dell'emergenza e Costituzione*, Napoli, 1982.

[94] Con questa espressione, autorevole dottrina intende evidenziare come la necessità di approntare strumenti di contrasto al fenomeno terroristico abbia finito per legittimare «scelte di politica penale nelle quali principi e garanzie proprie del diritto penale subiscono flessibilizzazioni che si muovono comunque in un'area limitrofa ad un confine pericoloso, quello al di là del quale si vanificano, in nome della ragion di Stato, garanzie e diritti individuali sui quali si fonda l'ordinamento democratico» (M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale al limite*, in *Quest. giust*., spec. 2016, p. 101).

[95] R.E. KOSTORIS, *Processo penale, delitto politico e «diritto penale del nemico»*, in *Riv. dir. proc.*, 2007, p. 4. In realtà, va dato conto che, perlomeno allo stato attuale, non vi è unanimità di pensiero in merito alla reale efficacia preventiva di questo tipo di investigazioni nel contesto delle attività di *intelligence*. Su questo aspetto, v. H. BOS-OLLERMAN, *Mass Surveillance and Oversight*, in D.D. Cole – F. Fabbrini – S. Schulhofer (a cura di), *Surveillance, Privacy and Trans-Atlantic Relations*, Oxford, 2017, p. 143.

Nel contesto della cd. *intelligence led policing*[96], dunque, non è certo casuale che i primi sistemi di *cyberpatrolling* – capaci, come detto, di operare una raccolta massiva di dati sfruttando la logica dei *big data* per finalità di *foreign intelligence*[97] – si siano andati sviluppando proprio nell'ambito delle attività realizzate dalle agenzie di pubblica sicurezza per il contrasto al terrorismo internazionale[98].

Per un verso, infatti, il concetto di sorveglianza contemporanea nasce proprio in ambito militare[99], nel quale il controllo costante delle attività altrui è alla base del buon funzionamento dell'apparato organizzativo di difesa. Per altro verso, la raccolta e l'analisi di informazioni volta alla prevenzione di possibili attentati alla sicurezza dello Stato costituisce, come detto, la funzione primaria dell'attività realizzata dai Servizi segreti.

Nel corso degli ultimi anni, però, si è assistito a un'espansione, a tratti incontrollata, delle attività di *intelligence* preventiva; un fenomeno che, a ben riflettere, appare strettamente connesso ai nuovi paradigmi offerti dalla *Information Technology* e, specialmente, alla diffusione delle nuove piattaforme di comunicazione[100]. Quando la vita pubblica si è spostata sui *social network*, i Servizi segreti hanno cominciato a svolgere attività di osservazione e raccolta occulta di informazioni in Rete[101]. Nell'ambito di una rinnovata centralità delle agenzie di *intelligence* nel nuovo scenario globale, l'attività di *cyberpatrolling* costituisce, dunque, la più evidente manifestazione di inedite logiche investigative[102].

Ciò nondimeno, il "pattugliamento *web* d'*intelligence*", come ogni sistema di sorveglianza digitale di massa «carente di trasparenza e della dovuta pubblicità»[103], rischia di minare le garanzie fondamentali degli individui, quantomeno laddove non sia sottoposto a adeguati controlli.

---

[96] Con tale espressione si allude comunemente a un nuovo paradigma di indagine che, nato nella metà degli anni '90 del secolo scorso nel contesto delle attività di polizia condotte nel Regno Unito, e sviluppatosi a seguito degli attenti terroristici avvenuti all'inizio del nuovo millennio, si fonda sull'analisi di tutte le informazioni disponibili e sulla collaborazione tra le forze dell'ordine, la comunità e i servizi di *intelligence* (così, J. RATCLIFFE, *Intelligence-Led Policing*, Cullompton, 2008, p. 8). La stretta connessione tra la diffusione di nuove metodologie di contrasto basate sull'*intelligence* e la tendenza all'aumento dell'osmosi tra l'ambito della prevenzione e quello della repressione è messa in evidenza da M. GIALUZ, *Banche dati europee e procedimento penale italiano*, cit., p. 253.

[97] G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Dir. inf. e informatica*, 2015, p. 25.

[98] Si veda, sul punto, il *report* redatto dal Governo inglese nel quale emerge, a chiare lettere, l'importanza assunta dalle attività di *intelligence* applicate ai *social network* nel contrasto al terrorismo nel Regno Unito (p. 169), *https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf*.

[99] D. LYON, *L'occhio elettronico*, cit., p. 48 s.

[100] Il dato è rilevato anche da T. NEWBURN – T. WILLIAMSONS – A. WRIGHT, *Handbook of Criminal Investigation*, Londra, 2008, p. 653.

[101] Lo afferma espressamente M. TESCONO, Big data *e* social media intelligence, in *Rivista italiana di intelligence*, 2017, p. 106: «i miliardi di iscritti alle piattaforme di *social networking*, generando ogni giorno un flusso costante di informazioni di portata inimmaginabile fino a pochi anni fa, costituiscono un 'occhio' sul mondo, un punto di osservazione sui fenomeni che accadono intorno a noi».

[102] Così definisce le tecniche di OSINT utilizzate dall'*intelligence*, D. CURTOTTI, *Procedimento penale e* intelligence, cit., p. 438.

[103] L. BACHMAIER WINTER, *Sorveglianza, indagati e diritti fondamentali: sfide nella lotta al terrorismo in UE*, in V. Militello – A. Spena (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Torino, 2018, p. 220.

A quest'ultimo proposito, non appare del tutto rassicurante l'approccio privilegiato dalla Corte europea dei diritti dell'uomo in tema di acquisizione e conservazione di dati su larga scala.

Dopo aver affermato – in maniera del tutto condivisibile – che le intercettazioni di massa sono «strumenti preziosi»[104] per la lotta al terrorismo, i giudici sottolineano che le autorità nazionali devono fornire garanzie idonee e adeguate contro l'arbitrarietà e il rischio di abusi, lasciando loro, però, un ampio margine di apprezzamento nell'individuare le misure più idonee a proteggere la sicurezza dei loro cittadini[105].

Esemplificativo, in tal senso, è l'obbligo imposto agli Stati contraenti di predisporre adeguati strumenti di controllo. Da un lato, infatti, viene sottolineata la necessità di un'autorizzazione preventiva o successiva da parte di un giudice o di un organo indipendente[106]; dall'altro, però, la Corte ha premura di precisare che l'assenza di tale meccanismo di garanzia non implica, di per sé, un superamento dei limiti di ciò che potrebbe essere ritenuto necessario «in una società democratica», omettendo di indicare, peraltro, quando la mancanza di controllo può considerarsi legittima[107], finendo così per «privilegiare del tutto ragioni di efficienza investigativa»[108].

Va emergendo, in questa prospettiva, una nuova categoria di soggetti, i cd. pre-indagati o potenziali sospettati[109], nei cui confronti l'operatività di una misura di controllo occulta e continuativa nell'ambito dei *social network* sembrerebbe, perlomeno a prima vista, contribuire a delineare un pre-giudizio di pericolosità sociale, in contrasto con il canone cristallizzato all'art. 27, comma 2, Cost.

Il tema, per la centralità che assume, merita qualche precisazione.

Tradizionalmente riferita alla condizione dell'imputato «nel corso del procedimento»[110], la presunzione di non colpevolezza è stata oggetto nel tempo di un'opera esegetica volta ad ampliarne lo spettro applicativo sotto il profilo della "durata". Con specifico riferimento al termine iniziale[111], più in particolare, ci si è chiesti se la presunzione di non colpevolezza «possa avere un qualche rilievo sul terreno della profilassi criminale»[112] in termini di regola

---

[104] Corte edu, 13 settembre 2018, *Big Brother Watch e altri c. Regno Unito*.

[105] Corte edu, 25 maggio 2021, *Centrum för rättvisa c. Svezia*.

[106] Nel contesto delle attività di *intelligence*, autorevole dottrina ha messo in rilievo come l'attività di controllo non debba essere affidata all'autorità giudiziaria – come da taluno prospettato –, bensì all'autorità governativa, la quale, in tal modo, verrebbe a esercitare «un tipico ruolo giudiziario, di tutela e garanzia dei diritti inviolabili». Diversamente opinando, si «finirebbe col confondere ancora di più le funzioni di polizia giudiziaria e di *intelligence*» (R. ORLANDI, *Attività di* intelligence *e diritto penale della prevenzione*, cit., p. 238).

[107] Corte edu, 13 settembre 2018, *Big Brother Watch e altri c. Regno Unito*, cit., par. 318 ss.

[108] Così si esprime, in proposito, D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, p. 32.

[109] L. BACHMAIER WINTER, *Sorveglianza, indagati e diritti fondamentali*, cit., p. 211.

[110] G. ILLUMINATI, *La presunzione di innocenza dell'imputato*, Bologna, 1979, p. 202.

[111] Con riguardo, invece, al termine finale, si registra, com'è noto, una diversità tra fonte costituzionale e fonte convenzionale. Mentre l'art. 27, comma 2, Cost., individua il momento ultimo di operatività della garanzia *de qua* alla sopravvenienza di una «condanna definitiva», l'art. 6, par. 2, CEDU, invece, si riferisce al raggiungimento della «prova legale della colpevolezza» che, perciò, potrebbe coincidere anche con una sentenza di primo grado. Su tale aspetto, anche per gli opportuni richiami dottrinali, si rinvia a P.P. PAULESU, *La presunzione di non colpevolezza dell'imputato*, cit., p. 78-88.

[112] P.P. PAULESU, *La presunzione di non colpevolezza dell'imputato*, cit., p. 105.

di trattamento ante-procedimentale, cioè prima e a prescindere dall'instaurarsi del rito. La questione, come noto, si è posta in relazione alle misure di prevenzione[113] e, più di recente, con riguardo sia alla disciplina sull'uso dei dati del codice di prenotazione dei passeggeri (PNR) ai fini della prevenzione e repressione del terrorismo e di altre gravi forme di criminalità[114], sia in merito al tema delle dichiarazioni di colpevolezza pre-procedimentali realizzate dall'autorità pubblica[115].

Facendo tesoro di quel fecondo dibattito, si potrebbe sostenere che «se […] è da considerarsi "non colpevole" l'imputato, *a fortiori* è da considerare tale anche il cittadino che non rivesta una qualità siffatta»[116] e che risulti sottoposto a misure di sorveglianza costante e continuativa *pre-iudicium*. Verrebbe enucleata, in tal modo, una regola universale di trattamento che postula l'illegittimità di qualunque «restrizione al godimento dei diritti fondamentali prima dell'instaurarsi del rito penale»[117].

Ancorché apprezzabilmente volta ad ampliare l'ambito di operatività della garanzia, un'esegesi di questo tipo rischia di indebolire il costrutto in parola, la cui applicazione generalizzata, in contrasto con una "concezione normativa" della presunzione di innocenza[118], potrebbe ridurne la portata garantista[119]. E proprio per evitare che quella «vocazione espansiva» si traduca in una «vocazione dispersiva»[120], una parte della dottrina ha messo in evidenza come la presunzione di non colpevolezza vada riferita esclusivamente

---

[113] Si veda, per una *summa* del dibattito, G. ILLUMINATI, *La presunzione di innocenza dell'imputato*, cit., p. 202 ss.

[114] Trattasi della Direttiva 2016/681/UE, recepita in Italia con il d.lgs. 21 maggio 2018, n. 53, la quale ha autorizzato il legislatore nazionale ad archiviare, elaborare e scambiare dati personali relativi ai passeggeri raccolti dalle compagnie aeree. Sul punto, la dottrina ha manifestato forti perplessità proprio con riguardo alla menomazione della presunzione di innocenza. Ogni singolo passeggero – si è sostenuto – sarebbe trattato con un pre-giudizio di pericolosità. Non solo, si è osservato, altresì, come «i dati raccolti in maniera indiscriminata e riversati in schedari pubblici accrescono la possibilità di incappare, per sbaglio, nelle maglie della giustizia, di essere ingiustamente accusati di reati, di subire rilevanti restrizioni di libertà fondamentali» (così, P. TROISI, *Dati PNR e trattamento pre-investigativo*, in A. Scalfati (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Torino, 2020, p. 331). Nello stesso senso, con riguardo al timore di un *vulnus* arrecato alla regola aurea sancita all'art. 27, comma 2, Cost., B. GALGANI, *Giudizio penale*, habeas data *e garanzie fondamentali*, in *Arch. pen.* web, 8 febbraio 2019, p. 19.

[115] Il riferimento è all'art. 4 della Direttiva 2016/343/UE del 9 marzo 2016 sul rafforzamento di alcuni aspetti della presunzione di innocenza, recentemente implementata in Italia ad opera del d.lgs. 8 novembre 2021, n. 188.

[116] Testualmente, A. BARBERA, *I principi costituzionali della libertà personale*, Milano, 1967, p. 229. Nello stesso senso, di recente, J. DELLA TORRE, *Ritratto di un'archiviazione come atto di (cripto)accusa*, in *Arch. pen.* web, 12 maggio 2021, p. 12, per il quale «in questa prospettiva il discrimine per valutare se o meno un soggetto sia titolare della presunzione non starebbe tanto nel profilo "formale" dell'avvio di un procedimento penale in senso stretto, quanto piuttosto nel fatto che un individuo sia sostanzialmente trattato come un colpevole dall'autorità, prima di essere condannato».

[117] Questa è la tesi sostenuta, sul punto, da W. NOCERINO, *Le intercettazioni e i controlli preventivi*, cit., p. 343. Nella stessa direzione sembra collocarsi pure L. BELVINI, *Principio di proporzionalità e attività investigativa*, Napoli, 2022, p. 106, nt. 72.

[118] Cfr. R. ORLANDI, *La duplice radice della presunzione di innocenza*, in *Riv. it. dir. proc. pen*., 2022, p. 627 ss.

[119] Questo è il timore espresso da R. ORLANDI, *La duplice radice della presunzione di innocenza*, cit., 636.

[120] Efficacemente, P.P. PAULESU, *La presunzione di non colpevolezza dell'imputato*, cit., p. 13. Su tale rischio, v. anche E. MARZADURI, *Considerazioni sul significato dell'art. 27, comma 2, Cost.: regola di trattamento e regola di giudizio*, in F.R. Dinacci (a cura di), *Processo penale e Costituzione*, Milano, 2010, p. 303 ss. e, spec., p. 306 s.

all'indagato o all'imputato[121], non anche al comune cittadino, nei confronti del quale l'ordinamento, mediante tecniche di *cyberpatrolling*, si limita a esercitare un «potere di prevenzione»[122], senza irrogare, invece, alcun tipo di sanzione[123]. In altri termini, non sembra ragionevole riferire il canone cristallizzato all'art. 27, comma 2, Cost. a un soggetto nei confronti del quale lo Stato non ha ancora esercitato lo *ius investigandi*. Diversamente opinando, la presunzione di non colpevolezza verrebbe surrettiziamente trasformata da cardine della giurisdizione penale a «principio di ordine pubblico»[124]. È in questa direzione, del resto, che pare muoversi anche la giurisprudenza europea laddove afferma, alla luce di una lettura restrittiva dell'art. 6, par. 2, CEDU, che la disposizione pattizia trova applicazione «*only when a criminal accusation is pending*»[125], escludendo, *de facto*, l'operatività *ante iudicium* della presunzione di innocenza.

Al netto di tale ultimo aspetto, la dottrina più accreditata ha messo in luce la necessità di approntare una disciplina generale in grado di contemperare i differenti interessi in gioco: sicurezza pubblica, da un lato, e tutela dei diritti fondamentali, dall'altro[126]. Specialmente con riguardo al contrasto al terrorismo, non può condividersi l'idea secondo cui la gravità del fenomeno giustificherebbe non solo un'attenuazione delle garanzie processuali, ma financo un'assoluta libertà investigativa[127].

Si obbietterà che questo tipo di *intelligence* criminale non è finalizzata alla produzione di prove spendibili in giudizio, bensì alla semplice prevenzione a tutela della sicurezza nazionale. Una tale affermazione, però, sarebbe fin troppo superficiale, quantomeno laddove si consideri che i dati raccolti nel corso di operazioni di *social network patrolling* possono

---

[121] E, difatti, si esprime in questi termini l'art. 27, comma 2, Cost.

[122] P.P. PAULESU, *La presunzione di non colpevolezza dell'imputato*, cit., p. 105.

[123] È proprio l'irrogazione di una "sanzione" (ancorché, ad avviso della dottrina maggioritaria, non strettamente penale), difatti, che giustifica l'operatività della presunzione di innocenza. Cfr., in tal senso, R. ORLANDI, *Procedimento di prevenzione e presunzione di innocenza*, in D. Negri – L. Zilletti (a cura di), *Nei limiti della Costituzione. Il codice repubblicano e il processo penale contemporaneo*, Milano, 2019, p. 94, ove sottolinea come «il principio previsto nell'art. 27 comma 2 Cost. (e nell'art. 6 comma 2 Conv. E.d.u.) è leso ogni volta che un soggetto è sottoposto a sanzione senza un previo, regolare e definitivo accertamento penale».

[124] P.P. PAULESU, *Contrasto al terrorismo e presunzione di non colpevolezza*, in *Riv. dir. proc*., 2008, p. 632.

[125] Corte EDU, 11 gennaio 2018, *Sharxhi e altri c. Albania*, par. 178.

[126] In tal senso, D. CURTOTTI, *Procedimento penale e* intelligence, cit., p. 448. Anche l'HM GOVERNMENT, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2010, p. 23, stabilisce che l'attività di SOCMINT deve essere svolta nel rispetto dei diritti umani e, specialmente, in ossequio ai principi di «*accountability, proportionality and necessity*».

[127] Del resto, in dottrina si è osservato come «la disciplina costituzionale del processo non ammette una diversificazione degli *standard* di garanzia in funzione dell'ipotesi accusatoria proprio perché, altrimenti, cadrebbe nell'insanabile contraddizione rappresentata dall'abbandono della presunzione di innocenza». Casomai, «volendo ammettere un certo margine di apprezzamento discrezionale da parte del legislatore […] l'unica equazione costituzionalmente e internazionalmente plausibile sarebbe quella di far corrispondere alla maggior gravità del reato oggetto di imputazione un incremento delle garanzie processuali dell'accusato» (O. MAZZA, *Tradimenti di un codice. La procedura penale a trent'anni dalla grande riforma*, Torino, 2020, p. 41 s.). Per una differente opinione, v., però, F. VIGANÒ, *Terrorismo, guerra e sistema penale*, cit., p. 648 ss. e, spec., p. 687-695, il quale argomenta muovendo dalla tesi secondo cui «le garanzie del diritto e del processo penale possono e debbono essere modulate diversamente a seconda della gravità e pericolosità dei fenomeni criminosi da contrastare». Sul punto, v. anche M. CHIAVARIO, *Garanzie ed efficienza della giustizia penale. Temi e problemi*, Torino, 1998, p. 14, il quale, pur sostenendo che «nessuna attenuazione dei diritti umani è prevista in diretto rapporto con l'oggetto del processo», ritiene «abbastanza giustificabile» la tendenza del legislatore processuale «ad adattare certe regole – più o meno direttamente legate alla dinamica di tali garanzie – con particolare riguardo ai delitti "di criminalità organizzata"».

essere legittimamente utilizzati, *de lege lata*, per portare avanti indagini penali o per «indirizzare le indagini verso una ricerca mirata»[128]; di fatto, nessuno può impedire che le informazioni raccolte in sede di *intelligence* siano successivamente utilizzate dalla polizia giudiziaria per lo svolgimento delle investigazioni. Se un tanto è vero, si dovrebbe ammettere che una determinata informazione acquisita mediate un controllo di massa – e, perciò, in violazione dei diritti fondamentali (ancorché, nel pieno rispetto della presunzione di innocenza) – pur non costituendo una prova, venga comunque utilizzata nell'ambito del procedimento: «non si tratta [forse] di un circolo vizioso?»[129].

Tutto ciò – si obietterà nuovamente – è del tutto naturale, come naturale è la tendenza dell'indagine penale a giovarsi, specialmente per il perseguimento di certe categorie di reati, di informazioni provenienti dall'attività di *intelligence*. Adottando un approccio di questo tipo, però, si corre il rischio di alimentare decisioni giudiziarie con dati e informazioni *extra* costituite e acquisite in violazione dei diritti fondamentali della persona[130], in aperto contrasto con il limite di natura epistemologica che caratterizza il rito penale. Come si è efficacemente osservato, infatti, il processo è – e deve rimanere – uno strumento «tendenzialmente impermeabile alle informazioni acquisite al di fuori di esso»[131].

6. "Ronde poliziesche virtuali" e prevenzione dei reati

Nell'esercizio della propria attività di prevenzione dei fenomeni criminosi, la polizia amministrativa e di sicurezza[132] ricorre sempre più frequentemente a operazioni di "pattugliamento nel *web*", finalizzate a individuare condotte illecite perpetrate tanto in ambito "digitale", quanto nel mondo "fisico", nonché a ricostruire l'evolversi di una determinata rete sociale di collegamenti, specialmente in relazione al crimine organizzato o

[128] W. NOCERINO, *Le intercettazioni e i controlli preventivi*, cit., p. 220, la quale esemplifica in questi termini: «si pensi, ad esempio, che sulla base delle notizie acquisite tramite intercettazioni preventive d'*intelligence*, pur non figurando negli atti di indagine, la polizia giudiziaria proceda a perquisizioni di propria iniziativa».

[129] Si pone questo interrogativo L. BACHMAIER WINTER, *Sorveglianza, indagati e diritti fondamentali*, cit., p. 221.

[130] Su tale rischio, v., *amplius*, D. NEGRI, *La regressione della procedura penale ad arnese poliziesco*, cit., p. 51.

[131] M.L. DI BITONTO, *Raccolta di informazioni e* attività di intelligence, cit., p. 257.

[132] Non è possibile soffermarsi, neppure brevemente, sull'antico (ma quantomai attuale) dibattito dottrinale in merito alla distinzione tra le funzioni di "polizia amministrativa" e quelle esercitate nell'ambito della "polizia di sicurezza". Per una completa rassegna delle diverse posizioni, v., per tutti, P. TONINI, *Polizia giudiziaria e magistratura*, cit., p. 249-251, il quale, all'esito dell'analisi condotta sul versante storico-normativo, afferma che «la polizia di sicurezza si può distinguere dalla polizia amministrativa in quanto concerne la tutela contro i pericoli e le turbative a interessi essenziali per la vita di una società civile quali l'ordine pubblico (in senso stretto) e la sicurezza delle persone e della proprietà» (p. 251).

cd. "di gruppo"[133]. Il cd. *ciberpatrullaje de seguridad*[134] è inteso, in questo ambito, come un insieme di tecniche e tecnologie che consentono di monitorare e controllare *ante delictum* le informazioni pubblicamente disponibili nei *social network*. Volendo ricorrere a un'analogia tra *physical world* e *virtual word*[135], può affermarsi che, così come le forze di sicurezza sorvegliano le strade delle città, parimenti, esse hanno cominciato a vigilare i cavi che collegano i dispositivi elettronici, luoghi di possibile commissione dei reati e fonti inesauribili di informazioni.

In tale contesto, le attività di *social network monitoring* costituiscono la frontiera della prevenzione penale del XXI secolo, come dimostrano accreditate ricerche, dalle quali emerge come, a partire dal 2012 nel sistema nordamericano[136] e dal 2015 in alcuni modelli europei[137], l'acquisizione di contenuti *open access* disponibili nei *social network* abbia cominciato a essere utilizzata in maniera sempre più frequente. Non stupisce, perciò, che nel 2018, ad esempio, il governo cileno abbia istituito un dipartimento specializzato della polizia (denominato OS-9) composto da ingegneri esperti che effettuano *ciberpatrullaje de carabineros* su diversi *social network*, con finalità di prevenzione delle condotte illecite perpetrate nel *web*[138]. Parimenti, l'autorità di pubblica sicurezza della Repubblica estone ha predisposto un progetto pilota, nel marzo 2021, per lo svolgimento di attività di *cyber*-pattugliamento dirette alla prevenzione dei delitti connessi al fenomeno dell'*hate speech*[139] e, più in generale, alla diffusione di contenuti illegali nella Rete[140]. Anche il governo canadese ha cominciato a impiegare strumenti di *cyberpatrolling* mediante l'uso di *software* in grado di raccogliere e trattare miliardi di dati in maniera automatizzata[141].

---

[133] Il riferimento è quegli studi sociologici e criminologici che, muovendo dall'idea secondo la quale i modelli di interazione sociale influenzano le condotte umane, sostengono che la comprensione delle dinamiche relazionali proprie delle strutture criminali complesse – come, ad esempio, quella mafiosa – ha un potenziale reale per scoprire le complessità delle reti intersoggettive. Si tratta, più in dettaglio, di attività che oggigiorno vengono sfruttate tanto in sede di *crime prevention*, quanto di *crime persecution*. Cfr., per approfondimenti, G. BERLUSCONI, *Social Network Analysis and Crime Prevention*, in B. Leclerc – E.U. Savona (a cura di), *Crime Prevention in the 21st Century. Insightful Approaches for Crime Prevention Initiative*, Cham, 2017, p. 129 ss.; M. CASTIELLO, *Reti criminali.* Social network analysis *e* criminal intelligence analysis. *Tecniche di contrasto a confronto*, Roma, 2015, *passim*; G. COSTABILE, *Le indagini digitali*, cit., p. 87-103, ove si riportano taluni casi pratici nei quali questa tecnica investigativa è risultata fondamentale per il buon esito delle indagini penali.

[134] Questa è l'espressione utilizzata in numerosi sistemi sudamericani (in specie, Argentina, Colombia, Brasile e Messico) nei quali, come si vedrà, l'impiego di simili strumentazioni è all'ordine del giorno (v. *https://datysoc.org/wp-content/uploads/2023/07/Informe-Ciberpatrullaje.pdf*). Cfr. *infra*.

[135] Cfr. Parte I, Cap. I, parr. 3, 4.

[136] L. EDWARDS – L. URQUHART, *Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?*, in *International Journal of Law and Information Technology*, 16 dicembre 2015, p. 8.

[137] D. TROTTIER, *Open Source Intelligence, Social Media and Law Enforcement: Visions, Constraints and Critiques*, in *European Journal of Cultural Studies*, 2015, p. 542.

[138] *https://www.latercera.com/nacional/noticia/desconocido-ciberpatrullaje-carabineros-lasredes-sociales/299027/*.

[139] *https://www.lrt.lt/en/news-in-english/19/1381641/lithuanian-police-to-patrol-social-media-send-facebook-messages-to-obvious-offenders*.

[140] *https://www.alfa.lt/straipsnis/50440147/troliai-ir-nepraustaburniai-slepkites-interneto-patruliai-pradeda-darba/*.

[141] Nell'ottica di garantire una maggiore trasparenza nello svolgimento di tali attività, il Parlamento ha reso pubblico l'elenco delle società private che prestano il loro servizio e le proprie strumentazioni tecnologiche a favore delle autorità di polizia (*https://www.vice.com/en/article/vvbpb9/the-canadian-government-told-us-its-down-with-social-media-monitoring*). Strumenti non dissimili, inoltre, sono stati implementati anche in

Tuttavia, è forse il sistema recentemente implementato in Argentina a costituire la più evidente manifestazione di quanto poc'anzi sostenuto. Il 2 giugno 2020, in piena emergenza pandemica, la Ministra della S*eguridad Nacional* ha adottato un *Protocoloco General para la prevenciòn policial del delito con usos de fuentes digitales abiertas*[142] con l'obiettivo di fornire una base giuridica per lo svolgimento di attività di *ciberpatrullaje* nelle «*redes sociales de cualquier ìndole*»[143]. Inizialmente circoscritto alla prevenzione di specifiche categorie delittuose, la genericità delle espressioni utilizzate in detto provvedimento («*detecciòn de posibles conductas delictivas*») ha consentito – e consente tutt'oggi – ai *cuerpos policiales* e alle *fuerzas de seguridad* di realizzare un monitoraggio e una vigilanza indiscriminata e sistematica di qualunque contenuto pubblico presente nello spazio digitale. Infatti, nonostante l'art. 8, comma 1, lett. f), del Protocollo vieti il ricorso al *ciberpatrullaje* per «monitorare e osservare a lungo individui o associazioni», l'ordito normativo pare comunque autorizzare una conservazione generalizzata dei contenuti *online*, salvo poi stabilire che quegli stessi dati dovranno essere distrutti nel caso in cui l'operazione non abbia dato luogo ad «*actuaciones judiciales*», cioè all'avvio di un procedimento penale[144].

Pur senza entrare nel dettaglio delle analitiche previsioni introdotte nei diversi ordinamenti stranieri or ora richiamati, è comunque possibile rilevare una certa propensione a implementare sistemi di controllo diffuso e occulto dei *social network*, giustificate dalla necessità di garantire un'efficace prevenzione di qualunque fenomeno criminoso realizzato sia *online* che *offline*.

Si tratta di una linea di tendenza, quest'ultima, che è possibile apprezzare anche sul versante italiano.

In realtà, nel panorama nazionale, l'espletamento di attività di prevenzione mediante "ronde digitali" volte all'apprensione di dati pubblici è stato perlopiù limitato – quantomeno in un primo momento – a settori specifici dell'ordinamento penale, caratterizzati da un allarme sociale ritenuto particolarmente significativo[145]: pedopornografia *online*, crimine

---

Indonesia (cfr. E.S. HASIBUAN, *The Role of Indonesian Police Throught "Cyber Patrol" in Preserving and Mantaining Cyber Room Security*, in *International Journal of Social Service and Research*, 2022, p. 722 ss.).

[142] *Resoluciòn* 144/2020. Il protocollo è stato aspramente criticato dalla dottrina argentina: cfr., in tal senso, A. LÒPEZ CABELLO – T.I. GRIFFA, *Privacidad en redes sociales y vigilancia estatal: un desafio pendiente de la pràctica constitucional argentina*, in *Anuario de derecho consitutcional latinoamericano*, 2020, p. 793 ss.; M. ARIEL GENDLER – I. RULLANSKY – F.L. ABIUSO, *Vigital y castigar en pandemia. Desafios teòrico-metodològicos en torno a la (in)definicòn del "ciberpatrullaje"*, in *Revista de la carrera de sociologìa*, 2022, p. 494 ss.; M. MONTE – S.I. SÀNCHEZ, *Tensiones constitucionales entre el derecho a la intimidad y el ciberpatrullaje en la investigación criminal. Análisis del Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas*, in *Revista pensamiento penal*, 23 aprile 2021.

[143] *Resoluciòn* 144/2020, cit.

[144] La *Resoluciòn* 144/2020, cit., enuclea così un vero e proprio «*principio de destruccion del material prevenido no judicializado*».

[145] Trattasi, dunque, di un'operazione che ben può essere classificata nell'ambito delle cd. *special investigative techniques*, cioè tecniche di indagine di tipo non convenzionale «che vengono regolamentate per contrastare illeciti rispetto ai quali le esigenze di repressione sono alimentate da un crescente allarme sociale […] ma soprattutto per penetrare nelle moderne organizzazioni criminali che, in determinati settori, si sono manifestate impenetrabili agli ordinari mezzi investigativi» (così, D. CURTOTTI, *"Le operazioni digitali sotto copertura": l'agente provocatore e l'attività di contrasto*, in AA.VV., Cyber Forensics *e indagini digitali*, cit., p. 505). D'altronde, come sottolinea A. APRUZZESE, *La recente normativa in tema di contrasto del terrorismo*, cit., p. 233, «tra i più efficaci strumenti di contrasto "precoce" di fenomenologie interessanti il *web* andrà posta quindi precipua attenzione alle cosiddette indagini proattive realizzate attraverso la cosiddetta OSint (*Open*

organizzato e terrorismo. Si è al cospetto, in effetti, di ambiti nei quali, per loro intrinseca natura, «la reazione più intelligente non è costituita dall'annullare le conseguenze di un atto, bensì […] dal prevenirlo»[146].

Con riferimento al primo, non potendo ripercorrere in questa sede la tortuosa evoluzione storico-normativa che ha portato all'adozione della l. 269/1998[147] volta a garantire una tutela ad ampio spettro dei soggetti minori, è sufficiente segnalare come le linee di intervento della novella si siano sviluppate tanto sul piano sostanziale – mediante l'introduzione di fattispecie *ad hoc*[148] – che processuale, attraverso la predisposizione di innovativi strumenti di prevenzione e repressione criminale. Tra questi, particolare attenzione merita l'istituto delle investigazioni digitali sotto copertura di cui all'art. 14, comma 2 della citata legge. La disposizione, com'è noto, consente al personale appartenente ai servizi di polizia postale di «utilizzare indicazioni di copertura, anche per attivare siti nelle reti, realizzare o gestire aree di comunicazione o scambio su reti o sistemi telematici, ovvero per partecipare ad esse». In termini non dissimili si esprime anche l'art. 9, comma 2, l. 146/2006[149] diretto a contrastare il crimine organizzato transnazionale, nella parte in cui consente agli ufficiali e agli agenti di polizia giudiziaria di utilizzare documenti, identità o indicazioni di copertura «per attivare o entrare in contatto con soggetti e siti nelle reti di comunicazione, informandone il pubblico ministero al più presto e comunque entro le quarantotto ore dall'inizio delle attività».

Orbene, entrambe le disposizioni, pur non facendo espresso riferimento a operazioni di *web patrolling*, sembrano presupporne, di fatto, l'esistenza. D'altro canto, non sarebbe immaginabile un'attività digitale sotto copertura senza una qualche preliminare analisi e perlustrazione generalizzata nella Rete[150]. Ciò nonostante, il legislatore non ha ritenuto opportuno disciplinarle *expressis verbis*, legittimando, *de iure condito*, forme di sorveglianza preventiva *ad libitum*[151].

Source Intelligence) […]. Le tecniche Osint al momento meglio si prestano a anticipare l'individuazione e il rilevamento di percorsi di radicalizzazione che non evidenziano ancora specifiche fattispecie penali».

[146] A. GARAPON, *Lo Stato minimo*, cit., p. 96.

[147] L. 3 agosto 1998, n. 269.

[148] Artt. 600-*ter*, 600-*quater*, 600-*quater1*, c.p.

[149] L. 16 marzo 2006, n. 146, con la quale l'ordinamento italiano ha ratificato e dato esecuzione alla Convenzione e ai Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 e il 31 maggio 2001. Trattasi della legge con la quale il Parlamento ha effettuato una vera e propria razionalizzazione delle attività *undercover*, ponendo fine alla proliferazione incontrollata di decreti-legge che fino all'epoca avevano governato la materia.

[150] Così, anche, F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., p. 98 s.; A. DEL PIZZO, *I crimini informatici a sfondo sessuale*, in M. Iaselli (a cura di), *Investigazioni digitali*, Milano, 2020, p. 530. Sulla natura "propedeutica" di tali attività, v., altresì, P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 80, il quale, però, sembra ritenere che esse siano state istituzionalizzate dal legislatore (p. 75), di talché non sarebbero ravvisabili frizioni sul versante della legalità processuale.

[151] A nulla varrebbe un eventuale richiamo al contenuto dell'art. 2-*bis* del d.l. 10 agosto 2023, n. 105 (conv. in l. 9 ottobre 2023, n. 137), con il quale il Parlamento ha modificato l'art. 9, comma 1, lett. b) della legge in parola e introdotto una nuova lett. b-*ter*). Stando alla disciplina di recente conio, gli ufficiali di polizia giudiziaria appartenenti agli organismi investigativi della Polizia di Stato e dell'Arma dei carabinieri, nonché, nel corso di operazioni di polizia finalizzate al contrasto dei reati informatici commessi ai danni delle infrastrutture critiche individuate dalla normativa nazionale e internazionale, gli ufficiali di polizia giudiziaria dell'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, possono introdursi all'interno di un sistema informatico o telematico, danneggiarlo, deteriorarlo, alterarlo o, comunque, compiere «attività prodromiche o strumentali». Quest'ultima locuzione, data la sua estrema genericità e

Il vuoto normativo, com'era prevedibile, è stato colto dalla giurisprudenza di legittimità che, onde garantire un più ampio margine operativo agli agenti di polizia, ha da tempo affermato che le operazioni di semplice «monitoraggio di siti *Internet*» finalizzate a visionare, scaricare e detenere *files* pedopornografici «liberamente disponibili al pubblico», non costituiscono vere e proprie "attività di contrasto" – che, in quanto tali, possono essere svolte solo dall'agente sotto copertura – e, quindi, non necessita dell'autorizzazione *ex* art.14 l. n. 269/1988[152].

Nella probabile consapevolezza di un grave *deficit* in termini di legalità processuale, il *lawmaker*, con riferimento al fenomeno terroristico, è intervenuto, invece, disciplinando appositamente una forma speciale di *cyberpatrolling*. In proposito, è noto come in questo settore le frontiere della prevenzione penale si muovano nel solco delle potenzialità offerte dalle nuove tecnologie. *Internet*, sotto tale profilo, ha offerto garanzie di anonimato e, contestualmente, una diffusività capillare delle informazioni, elemento, quest'ultimo, funzionale allo svolgimento di attività di propaganda e reclutamento. La Rete, in tal senso, ha fornito le infrastrutture tecniche per ciò che è stata efficacemente definita «globalizzazione del terrorismo»[153].

Nella ragionevole convinzione che il fenomeno *de quo* agisce prevalentemente "in linea", il legislatore italiano ha predisposto, perciò, una serie di misure e tecniche investigative di natura digitale aventi al contempo finalità preventiva e repressiva[154]. D'altronde, è stato osservato come lo sviluppo di attività di indagine incentrate sull'apprensione di dati e informazioni – e, più in generale, sul rafforzamento dell'ampio ventaglio di misure riconducibili al settore della *digital surveillance* – costituisca il «*trend* comune»[155] di ogni legislazione processuale in materia di antiterrorismo.

È in questo contesto che si colloca l'art. 2 del d.l. 7/2015[156]. La disposizione introduce una vera e propria «forma di indagin[e] occult[a]»[157] rappresentata dal monitoraggio

---

l'assenza di qualunque limite temporale, oggettivo e soggettivo, non sembra in grado di offrire alcuna una copertura legislativa all'attività di *cyberpatrolling*.

[152] Cass. pen., Sez. III, 30 ottobre 2009, n. 41743; Cass. pen., Sez. III, 5 febbraio 2009, n. 13729; Cass. pen., Sez. V, 19 gennaio 2004, n. 21778; Cass. pen., 11 febbraio 2002, n. 5397.

[153] A. GARAPON, *Lo Stato minimo*, cit., p. 59.

[154] M. DANIELE, *Le indagini informatiche contro il terrorismo bilanciamenti difficili e timori legislativi*, in R. Wenin – G. Fornasari (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, Trento, 2017, p. 265, per il quale «il terrorismo e le indagini informatiche rappresentano una coppia indissolubile nell'era della globalizzazione. Si evolvono di pari passo. Più il terrorismo, grazie alle tecnologie digitali e all'uso delle reti informatiche, espande la sua capacità di reclutamento e la sua forza letale, più, parallelamente, le indagini informatiche si raffinano e ampliano la loro valenza repressiva».

[155] G. DI PAOLO, *Nuove sfide tra terrorismo, sviluppo tecnologico e garanzie fondamentali: note introduttive*, in R. Wenin – G. Fornasari (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, cit., p. 244, la quale soggiunge come «in buona sostanza, si risponde al "terrore globale" instaurando una sorta di controllo globale, di orwelliana memoria».

[156] D.l. 18 febbraio 2015, n. 7, convertito in legge 17 aprile 2015, n. 43, recante misure urgenti per il contrasto al terrorismo, anche di matrice internazionale. Per un commento alla normativa, cfr. S. SIGNORATO, *Le misure di contrasto in rete al terrorismo:* black list, *inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio* Internet, in R.E. Kostoris – F. Viganò (a cura di), *Il nuovo "pacchetto" antiterrorismo*, Torino, 2015, p. 55 ss.

[157] Così definisce il *cyberpatrolling* in questo contesto, M. DANIELE, *Le indagini informatiche contro il terrorismo*, cit., p. 270, nt. 16.

continuativo e massivo dei siti *Internet* utilizzati da potenziali terroristi. Più nel dettaglio, il costrutto normativo autorizza la polizia di sicurezza (e, invero, anche la polizia giudiziaria[158]) a compiere di propria iniziativa manovre di perlustrazione a tappeto del *web* finalizzate alla prevenzione del fenomeno terroristico, a prescindere da qualsiasi provvedimento autorizzatorio del pubblico ministero. L'attività, più in particolare, è finalizzata alla successiva predisposizione, a opera degli apparati di pubblica sicurezza presso il Ministero dell'interno[159], di un elenco di siti *internet* (cd. *black list*) utilizzati dai presunti terroristi per la realizzazione delle condotte previste agli artt. 270-*bis* e 270-*sexies* c.p.[160].

A tal proposito, non si può fondatamente dubitare che tali operazioni possano essere legittimamente compiute anche nei *social network*; d'altro canto, sarebbe irragionevole, nonché in contrasto con la *ratio legis* della novella, impedire all'autorità di pubblica sicurezza di pattugliare quei canali digitali di comunicazione che costituiscono oggigiorno il "luogo" nel quale vengono perpetrare la maggior parte delle condotte di proselitismo e apologia legate al fenomeno *de quo agitur*. A sconfessare eventuali tesi contrarie (da taluno sostenute[161]), muove una considerazione di carattere letterale. L'oggetto dell'attività di pattugliamento viene normativamente individuato nei «siti» utilizzati per le attività terroristiche, ovverosia "pagine" *web* impiegate con finalità illecite; un concetto, quest'ultimo, al quale debbono essere ricondotte le moderne piattaforme digitali di comunicazione, anche qualora il loro utilizzo avvenga – come spesso accade – per mezzo di applicazioni mobili (*applications*) installate sullo *smartphone* o sul *computer*. In questi casi, infatti, il segnale *Internet* risulta comunque indispensabile per collegarsi al dominio del *provider* e, cioè, ad un «sito» (ad esempio, *www.facebook.com*).

Al netto di tale aspetto, e nonostante l'apprezzabile sforzo del legislatore processuale nell'aver espressamente cristallizzato forme di sistematica perlustrazione del *web*, deve comunque rilevarsi, anche in questa sede, un significativo *deficit* di legalità. Nulla è detto, infatti, in merito alle modalità, alle tempistiche e ai caratteri di tale sorveglianza. Il messaggio del legislatore, a tal proposito, è sfacciatamente cristallino: le esigenze di prevenzione del crimine organizzato, del terrorismo e della pedopornografia giustificano forme di *digital mass surveillance*.

Preso atto, dunque, delle numerose potenzialità sottese a questa nuova tecnica di indagine e del vuoto normativo in materia, non v'è da stupirsi se le autorità di *law enforcement* hanno cominciato a interrogarsi sulla possibilità di sfruttare simili meccanismi anche al di fuori

---

[158] Come sottolinea D. NEGRI, *La regressione della procedura penale ad arnese poliziesco*, cit., p. 49, nel caso di specie il legislatore «profitta dell'immedesimazione organica dovuta al ruolo bifronte del personale appartenente alla Polizia postale e delle comunicazioni, appunto incaricato un decennio addietro sia della "prevenzione" sia della "repressione" dei reati di natura terroristica commessi con mezzi informatici (art. 7-bis, d.l. n. 144 del 2005)».

[159] Il riferimento va inteso al Servizio di Polizia Postale e delle comunicazioni, oggi denominato Centro Nazionale per la Sicurezza Cibernetica.

[160] A tal proposito, la disciplina ha istituito una sorta di misura cautelare *ad hoc*, prevedendo che l'autorità giudiziaria procedente possa obbligare gli ISP a inibire l'accesso ai siti contenuti in detta "lista nera".

[161] Per i dovuti richiami, si rinvia a L. VIOLA BERRUTI, Black list *e blocco dei contenuti* web *illeciti: dal contrasto alla pedopornografia al* cyber terrorism, in *Leg. pen.* web, 15 gennaio 2016, p. 4.

delle ipotesi espressamente previste dalla legge[162]. Più in particolare, il dilagare della delinquenza *online* e la presa d'atto che i *social network* costituiscono una delle principali "banche dati investigative"[163] dell'era moderna ha indotto la polizia di sicurezza a implementare forme di sorveglianza digitale, nell'intento di individuare qualunque tipologia di condotta illecita perpetrata nel *web*, nonché acquisire il maggior numero di informazioni disponibili in Rete. Nell'ottica di una prevenzione digitale a 360 gradi, numerose Sezioni Operative del Centro Nazionale per la Sicurezza Cibernetica hanno già incardinato, all'interno dei propri Dipartimenti, uffici specializzati nel condurre attività di monitoraggio dei contenuti *open access* pubblicati nelle principali piattaforme digitali[164]. Agenti di polizia altamente specializzati vengono oggigiorno assegnati allo svolgimento di operazioni di *web patrolling*. Ancorché si tratti di progetti talvolta in via di sviluppo – e rilevato che l'esperienza insegna che «le nuove tecniche investigative tendono ad essere impiegate prima che ne siano disciplinate le modalità, anche quando sono in gioco diritti individuali che la legge dovrebbe tutelare»[165] – non è difficile immaginare che nell'arco di pochi anni ogni Dipartimento distaccato a livello periferico della Polizia postale sarà dotato di una Sezione specializzata in *social network monitoring*.

La creazione di un *cyber*-poliziotto 2.0 quale "sentinella dormiente"[166] del *cyberspace*, dunque, è già realtà[167].

Tuttavia, la liberalizzazione nella prassi di simili attività non è stata accompagnata da una presa d'atto in sede legislativa: il *cyberpatrolling* preventivo è un'operazione di polizia attualmente orfana di regole. Trattandosi di uno specifico strumento di sorveglianza digitale, però, tanto le fonti europee (come, ad esempio, la Raccomandazione del Comitato dei Ministri CM/Rec(2014)4 sulla sorveglianza elettronica), quanto taluni documenti di *soft law* a livello internazionale, consentono agli Stati di introdurre misure di controllo attivo sui propri cittadini solo qualora vi sia una legge chiara e precisa che, nel rispetto del principio di proporzionalità, indichi i tipi, la durata e le modalità di esecuzione del controllo[168].

---

[162] Si consideri, a mero titolo esemplificativo, l'attività di prevenzione dei cd. *flash mob* illegali o le operazioni di contrasto ai fenomeni illeciti connessi alle *fake news*.

[163] In questo contesto, l'espressione è utilizzata non tanto per riferirsi alla "banca dati" quale «strumento di trasmissione di un provvedimento o di una richiesta emessa nel corso di un procedimento giudiziario», bensì come «contenitore di informazioni che possono essere utili per l'accertamento dei fatti e delle responsabilità. In quest'ottica, è il procedimento penale a essere destinatario di dati immagazzinati in archivi informatici» (per tale classificazione, v. M. GIALUZ, *Banche dati europee e procedimento penale italiano*, cit., p. 236).

[164] *https://www.ilmattino.it/napoli/cronaca/web_patrolling_carabinieri_napoli_ultime_notizie_oggi-7115531.html*; *https://www.labussolanews.it/2022/12/15/napoli-carabinieri-web-patrolling-social/*; *https://www.giustizianews24.it/2022/12/15/web-patrolling-lultima-frontiera-dei-carabinieri-a-napoli-un-nucleo-setaccia-la-rete-a-caccia-di-boss-latitanti-e-babygang/*.

[165] R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 132.

[166] L'icastica espressione è mutuata da F. BUENO DE MATA, *Investigación y prueba de delitos de odio en Redes Sociales*, cit., p. 178 (trad. nostra).

[167] Ed è proprio per questa ragione, a ben riflettere, che F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Proc. pen. giust*., 2017, p. 195, mette in guardia dal rischio di «assuefarci all'idea di un "poliziotto digitale" che, arbitrariamente e sprovvisto di regole che ne governino l'incedere, s'insinui nel cyberspazio all'inseguimento incontrollato del "cittadino digitale"».

[168] Cfr., rispettivamente, la Raccomandazione del Comitato dei Ministri CM/Rec(2014), 19 febbraio 2014, par. III, punto 1 e il *report* pubblicato dalle Nazioni Unite nel 2019, reperibile al sito *https://news.un.org/es/story/2019/06/1458401*.

Pertanto, se può ragionevolmente comprendersi, *de lege lata*, l'assenza di una disciplina codicista – posto che trattasi di funzioni esercitate nell'ambito della polizia amministrativa e, perciò, in un momento antecedente all'inizio formale del procedimento –, assai meno giustificabile appare, invece, la scelta del legislatore di disinteressarsi *in toto* del fenomeno *de quo*[169]. Mette conto sottolineare, in proposito, che la stessa giurisprudenza di legittimità ha avuto modo di osservare come la «realizzazione di indagini a tappeto ed in forma indiscriminata», dirette ad accertare se ipotetici reati siano stati commessi «è consentita soltanto agli organi di polizia nell'esercizio della propria attività amministrativa di prevenzione»; un'attività, però, – proseguono i giudici – che, in quanto svolta al di fuori delle norme del codice di rito, va effettuata comunque «nel pieno rispetto delle altrui libertà»[170].

Il *punctum dolens*, dunque, riguarda la mancata individuazione di limiti allo svolgimento di un'operazione che appare lesiva dei diritti fondamentali della persona. Il *vulnus* arrecato alla riservatezza e il *chilling effect* originato da semplice timore di essere sottoposti a controllo da parte delle autorità pubbliche rendono necessaria l'apposizione di restrizioni ben definite.

In realtà, la scelta di rinunciare all'adozione di una disciplina *ad hoc* potrebbe essere giustificata invocando un'analogia tra l'attività di *preventive social network monitoring* e le operazioni di pattugliamento nel mondo fisico: nello stesso modo in cui la legge consente alla polizia amministrativa di vigilare liberamente le strade delle città (art. 1, comma 2, r.d. 18 giugno 1931, n. 773[171]), realizzando così un'attività di prevenzione, parimenti, la nuova realtà socio-digitale obbliga le autorità di *law enforcement* a porre in essere la medesima operazione nel contesto virtuale[172]. Di conseguenza, l'atto in questione ben potrebbe essere classificato come una semplice modalità "tecnologicamente avanzata" di pedinamento tradizionale[173]: un rapporto, dunque, di *genus* a *species*. Diversamente opinando, l'ordinamento non sarebbe in grado di garantire un'efficace prevenzione non solo con riguardo alla criminalità *online*, ma anche in relazione a quella tradizionale, posto che le informazioni reperibili sui *social network* possono essere utilizzate anche con riguardo alla

[169] Sul punto, v. le condivisibili considerazioni di F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., p. 97, il quale mette in luce come «non diversamente da quanto avviene per il controllo *ab initio* rivolto verso un determinato bersaglio, anche le operazioni [di vigilanza massiva] sono in grado di provocare un *vulnus* alle prerogative individuali, se non altro poiché finiscono per coartare il diritto all'autodeterminazione delle persone anche solo potenzialmente interessate dalla misura».

[170] Cass. pen., Sez. III, 26 gennaio 1999, n. 3261.

[171] Trattasi del Testo unico delle leggi di pubblica sicurezza, in base al quale «l'autorità di pubblica sicurezza veglia al mantenimento dell'ordine pubblico, alla sicurezza dei cittadini, alla loro incolumità e alla tutela della proprietà; cura l'osservanza delle leggi e dei regolamenti generali e speciali dello Stato, delle provincie e dei comuni, nonché delle ordinanze delle Autorità; presta soccorso nel caso di pubblici e privati infortuni».

[172] Nell'accogliere questa lettura, A. APRUZZESE, *La recente normativa in tema di contrasto del terrorismo*, cit., p. 234, parla di un «vecchio poliziotto "di strada" che vigila e osserva oltre che nelle pubbliche strade anche in contesti oscuri e mascherati».

[173] La tesi chiama alla mente il parallelismo operato dalla giurisprudenza di legittimità in relazione al rapporto tra pedinamento tradizionale e pedinamento elettronico. In quel contesto, infatti, i giudici hanno più volte sottolineato come l'impiego del *tracker* GPS costituisca una «modalità peculiare e tecnicamente avanzata» dell'attività di osservazione dei movimenti dell'indagato (o di terzi) svolta dalle forze dell'ordine (cfr., *in primis*, Cass. pen., Sez. V, 27 febbraio 2002, Bresciani).

criminalità ordinaria. Questo *modus interpretandi*, peraltro, è stato avallato pure in altri ordinamenti. In mancanza di una disciplina *ad hoc*, la *Sala de lo penal* del *Tribunal Supremo* spagnolo, ad esempio, ha recentemente stabilito che le forze di polizia possono compiere legittimamente, pur in assenza di un'autorizzazione previa, qualunque attività di «*rastreo en las redes sociales publicas*», giacché questa rientra a pieno titolo nelle funzioni legalmente attribuite «*a las Fuerzas y Cuerpos de Seguridad del Estado*», tra le quali rientrano anche la prevenzione e la repressione dei reati[174].

Il ricorso a un'interpretazione estensiva, per quanto possa a prima vista apparire funzionale alla tutela della sicurezza pubblica, non sembra pienamente convincente.

Anzitutto, un tale *modus argomentandi* è destinato a entrare in frizione con il principio di legalità, inteso quale «diritto del singolo di conoscere le ragioni per le quali subisce una restrizione della sua sfera di libertà, nonché le modalità con cui la stessa si realizza»[175], indipendentemente dall'instaurarsi di un procedimento penale. In assenza di una regolamentazione specifica, l'attività di prevenzione digitale è priva di limiti, cosicché chiunque potrebbe astrattamente divenire bersaglio di *cyberpatrolling*.

Ma ciò che desta maggiori perplessità è la mancata considerazione della differenza qualitativa tra le attività a confronto.

Il "pattugliamento fisico" è operazione che va incontro a una serie significativa di limitazioni e difficoltà pratiche legate ai costi, ai tempi, all'impiego di personale, ai rischi che gli agenti possano essere scoperti e a eventuali barriere fisiche che possono frapporsi tra il controllato e il controllore, nonché, da ultimo, alla ridotta capacità di analisi delle informazioni raccolte. Al contrario, l'attività di vigilanza nel contesto dei *social network* è «quasi impercettibile»[176] e implica non solo una semplice raccolta di dati, ma anche la possibilità di incrociare in maniera automatizzata tutte le informazioni acquisite[177].

Si obietterà – richiamando un'argomentazione già spesa dalla dottrina americana a sostegno della legittimità di un uso capillare delle videocamere di sorveglianza nei luoghi pubblici[178] – che l'attività di prevenzione realizzata mediante *cyberpatrolling* costituisce, in realtà, una sorta di equivalente tecnologico di centinaia di poliziotti intenti a spiare gli individui in ogni attimo della loro vita *online*.

La censura, comunque la si voglia intendere, non coglierebbe nel segno.

Occorre sottolineare, infatti, che l'attributo tecnologico proprio di un determinato mezzo di ricerca della prova non incide esclusivamente sul versante delle sue concrete modalità esecutive, bensì, volendo ricorrere a un linguaggio proprio degli studiosi di diritto penale

---

[174] Tribunale Supremo spagnolo, 17 marzo 2017, n. 11, ove si afferma testualmente che «*las fuerzas y cuerpos de seguridad patrullan por la Red* [*y por las redes sociales*] *del mismo modo que sus agentes patrullan por las calles*»; Tribunale supremo spagnolo, 1° marzo 2016, n. 4.

[175] W. NOCERINO, *Le intercettazioni e i controlli preventivi*, cit., p. 345.

[176] Così, R. LEVINSON-WALDMAN, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, in *Howard Law Journal*, 2018, p. 534 (trad. nostra).

[177] La circostanza che l'impiego di *software* in grado di operare "automaticamente" su dati grezzi abbia prodotto un "salto qualitativo" nello svolgimento delle operazioni investigative e di prevenzione è messo chiaramente in luce da R. ORLANDI, *Uso poliziesco dell'intelligenza artificiale. L'insegnamento del* Bundesverfassungsgericht, in *Cass. pen.*, 2023, p. 2174.

[178] Il dibattito è ampiamente esaminato da G. DI PAOLO, *"Tecnologie del controllo" e prova* penale, cit., p. 146 ss., alla quale si rinvia anche per i dovuti riferimenti bibliografici.

sostanziale, risulta un elemento "specializzate" della fattispecie, tale da provocarne un "salto di qualità" in grado di implementarne l'efficacia. La condotta dell'agente (o degli agenti) in borghese che realizzano pattugliamenti *on the street* è qualitativamente diversa dalla tecnica di *social network patrolling*, raffinata operazione di sorveglianza offerta dall'innovazione tecnologica[179].

Le due attività, inoltre, sembrano distinguersi anche sotto un profilo quantitativo.

Com'è stato acutamente osservato, uno dei fattori che contribuisce a differenziare l'esperienza reale da quella virtuale è la componente temporale[180]: il carattere immanente dei dati presenti in Rete, infatti, consente loro di permanere per sempre nel cyberspazio, indipendentemente dalla volontà di chi li ha "caricati" nella Rete[181]. In questa prospettiva, si comprende come il *cyberpatrolling* consenta alle forze di sicurezza di acquisire (e, successivamente, trattare, grazie all'impiego di *software* di IA) una grande mole di dati e informazioni che possono astrattamente «coprire l'intera esistenza digitale del soggetto, dando vita ad una sorta di "*time machine*" investigativa»[182]. Ma, com'è stato efficacemente osservato, «oltre una certa misura, il problema da quantitativo diventa [nuovamente] qualitativo»[183].

---

[179] Si vedano, benché in altro contesto, le considerazioni di A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen*., 2005, p. 634. Sulla capacità del formante tecnologico di mutare i connotati strutturali di una tecnica investigativa, v., più di recente, F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., p. 70-76. Sul punto, può essere utile ricordare il dibattito sorto in merito al rapporto tra pedinamento tradizionale e *tracker* GPS. I fautori della tesi maggioritaria sottolineano come la componente tecnologica propria della geolocalizzazione determini una compressione delle libertà individuali maggiore rispetto al pedinamento ordinario (S. MARCOLINI, *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, p. 2867; C. FANUELE, *La localizzazione satellitare nelle investigazioni penali*, Milano, 2019, p. 8, 11; T. BENE, *Il pedinamento elettronico: tecnica investigativa e tutela dei diritti fondamentali*, in A. Scalfati (a cura di), *Le indagini atipiche*, cit., p. 443 ss.; C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, p. 240). Altra postura dottrinale, invece, ritiene che, a parità di durata, il pedinamento tradizionale risulti più invasivo, poiché consente di cogliere tutta una serie di elementi ulteriori, quali, ad esempio, la gestualità del bersaglio (così, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 291).

[180] V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Rivista di diritto dei media*, 2018, 2, p. 32.

[181] V., ancora, V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari*, cit., p. 32, per il quale «mentre nel mondo reale esiste il passato, nel mondo digitale ogni elemento è sempre presente perché ne conserviamo una traccia». A tal proposito, la stessa EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA) ha pubblicato un documento (*Security issues and Recommendations for on line social networks*, 2007) nel quale si sottolinea che, mentre i profili *social* di un utente possono essere modificati o cancellati, non è possibile impedire che i dati *ivi* pubblicati siano memorizzati altrove, assumendo così «una vita propria» (p. 8).

[182] In questi termini, P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 87, il quale alla nt. 63, richiama l'efficace metafora, di matrice statunitense, di un'indagine penale che «viaggia nel tempo». Più in generale, sulla capacità dei moderni *investigative tools* di consentire alle autorità inquirenti l'accesso all'«intera esistenza digitale delle persone», v. M. DANIELE, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. pen. giust*., 2018, p. 834.

[183] R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, p. 1153, nt. 52, il quale ricorda come la stessa Corte costituzionale tedesca, nella storica sentenza del 1983 con la quale riconobbe il "diritto alla autodeterminazione informativa", ebbe a sottolineare che l'avvento di nuove tecnologie in grado di ricercare e archiviare una massa enorme di dati costituisse un inedito pericolo per la libertà degli individui (Bundesverfassungsgericht, 15 dicembre 1983 n. 65).

6.1 Sorveglianza nei *social network* e pre-inchiesta: l'art. 330 c.p.p. come limite allo svolgimento di operazioni investigative *online* lesive del diritto alla riservatezza

Le considerazioni appena svolte consentono di affermare, senza timore di smentita, che il *cyberpatrolling* rappresenta un nuovo modo di concepire e attuare la prevenzione penale. Più in particolare, la sua natura intrinsecamente esplorativa, in combinato congiunto con l'applicazione di strumentazioni di intelligenza artificiale, rischia di dar vita non tanto ad attività di "pattugliamento amministrativo" *ante notitia criminis* – come tali giustificate, a determinate condizioni, dalla necessità di garantire la *tranquillitas* collettiva –, bensì a vere e proprie operazioni investigative finalizzate alla ricerca di "una" notizia di reato (cd. indagini proattive o investigazioni pre-procedimentali)[184].

Se è ben vero, come ammonisce attenta dottrina, che «pensare ad un procedimento penale che si instaura con l'acquisizione della *notitia criminis* è immagine alquanto anacronistica e sicuramente poco aderente alla realtà»[185], nondimeno, non possono essere sottaciuti i rischi che si celano dietro a un ricorso privo di limiti di una sorveglianza pre-investigativa, tanto nel caso di *cyberpatrolling* non targettizzato, quanto di *screening* individualizzato. Con riferimento a quest'ultima ipotesi, tornano ad affiorare, pure in tale contesto, i timori per il possibile riproporsi di quell'*inquisitio generalis* che la dottrina più autorevole aveva messo in luce con riguardo al fenomeno della criminalità organizzata *lato sensu* intesa già a metà degli anni '90 dello scorso secolo[186].

Il tema al quali si allude, come noto, è quello delle investigazioni preliminari alla stessa indagine preliminare, operazioni che, legittimate dalla *littera* dell'art. 330 c.p.p.[187], si collocano da sempre in una "zona grigia", non disciplinata dalla legge[188], al confine tra la prevenzione e la repressione. Quale *tertium genus* e in assenza di una formale iscrizione *ex* art. 333 c.p.p., la fase della pre-inchiesta assume una natura ibrida, né amministrativa, né *stricto sensu* giudiziaria-procedimentale.

---

[184] Mettono in luce tale rischio con riguardo, più in generale, alle attività di sorveglianza continuativa quali forme di investigazione penale esplorativa, F. SIRACUSANO, *La prova informatica transnazionale*, cit., p. 181; P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 21.

[185] F. GIUNCHEDI, *Le attività di prevenzione e di ricerca di* intelligence, cit., p. 1. Non può negarsi, in effetti, che «la notizia della commissione di un reato emerge solitamente nell'ambito delle attività di osservazione, informazione e vigilanza compiute durante i servizi di prevenzione», L. D'AMBROSIO, *Ruolo e attività della polizia giudiziaria nelle indagini: brevi considerazioni e qualche proposta*, in *Cass. pen.*, 2006, p. 2686.

[186] R. ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis?, in *Riv. it. dir. proc. pen.*, 1996, p. 581, il quale sottolinea come «specialmente nella lotta contro il crimine organizzato, molte attività qualificate come "preventive" sono, con tutta evidenza, piegate a scopi prevenivi» (p. 584).

[187] In generale, la disposizione, discostandosi in parte dall'art. 219 c.p.p. 1930, individua due differenti modalità mediante le quali tanto il pubblico ministero quanto la polizia giudiziaria possono acquisire la *notitia criminis*: ricezione e apprensione. Se, nel primo caso, gli organi d'accusa svolgono un ruolo meramente passivo, nel secondo, invece, la possibilità di «prendere notizia dei reati di propria iniziativa» configura una vera e propria fase pre-investigativa nella quale si è chiamati a vagliare la traducibilità delle informazioni raccolte in una vera e propria notizia di reato.

[188] L'assenza di una disciplina è dovuta alla scelta dei *conditores* del 1988 di ancorare l'avvio formale del procedimento penale all'iscrizione della notizia di reato nell'apposito registro *ex* art. 335 c.p.p. Per tale ragione, dunque, il codice di rito non detta alcuna regolamentazione né con riguardo ai tempi, né in relazione agli strumenti utilizzabili in detta fase. Ciò nonostante, la dottrina più attenta sottolinea da tempo la necessità di approntare un *corpus* di garanzie a fronte dello svolgimento di attività investigative pre-procedimentali (sul punto, v., per tutti, P.P. PAULESU, *Notizia di reato e scenari investigativi complessi: criminalità organizzata, indagini sotto copertura, captazione di dati digitali*, in *Riv. dir. proc.*, 2010, p. 803).

Ciò nonostante, la rilevanza per il processualpenalista del tema è dovuta al fatto che la notizia di reato, in questo contesto, «cessa di essere un mero presupposto di fatto del procedimento penale», configurandosi, invece, come «un atto conclusivo dell'inchiesta preparatoria»[189]. Le attività realizzate in questa fase soggiacciono alle leggi e ai limiti propri della polizia amministrativa, ma, in concreto, perseguono finalità legate alla repressione, poiché poste in essere in un momento successivo alla commissione di un illecito, ma prima che lo stesso venga qualificato in termini di vera e propria notizia di reato. Quest'ultima, allora, lungi dal costituire uno spartiacque tra due momenti concettualmente distinti[190], assume i contorni di un «accidente giuridico»[191] che legittima indirettamente l'idea di una linea di continuità investigativa, un'omogeneità tra ciò che accade prima e ciò che accade dopo[192]. E, in effetti, colgono nel segno quegli autori che sottolineano come la funzione investigativa sia sostanzialmente unitaria e, di fatto, indivisibile, giacché nella maggior parte dei casi l'attività di polizia giudiziaria costituisce una sorta di "progressione ideale" dell'attività di polizia amministrativa, nel senso che la notizia di reato emerge nell'ambito di operazioni compiute nel corso di servizi di prevenzione[193].

Alla luce delle suesposte considerazioni, appare evidente come anche nel *cyberpatrolling* il confine tra vigilanza amministrativa e sorveglianza pre-investigativa avente carattere esplorativo appaia evanescente e sfuggevole. In maniera assai più marcata rispetto a quanto è dato riscontrare nel contesto delle indagini digitali (e, in particolare, delle perquisizioni informatiche[194]), le operazioni di *social network monitoring* rendono sfumata la distinzione tra prevenzione e repressione, potendo le stesse degenerare in strumenti «di ricerca di altre, nuove notizie di reato», consentendo così all'autorità procedente di ricercare «ciò che vuole, non quel che deve»[195]. Il rischio, evidentemente, è quello di legittimare operazioni di ricerca della prova non delimitate solamente all'addebito contestato, dando corso a un reperimento incessante e continuo di notizie di reato che, in un sistema governato dall'obbligatorietà

[189] R. ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata*, cit., p. 589. Anche secondo P. TONINI, *Polizia giudiziaria e magistratura*, cit., p. 1, la fase pre-procedimentale pone «questioni che non sono di carattere meramente burocratico-amministrativo, ma che toccano aspetti essenziali della disciplina del processo penale».

[190] Perché distinte sono le funzioni attribuite alla "polizia" nella fase di prevenzione e nella fase di repressione.

[191] F. DE LEO, *Il pubblico ministero tra completezza investigativa e ricerca dei reati*, in *Cass. pen.*, 1995, p. 1441, il quale considera «tutta la fase investigativa antecedente all'azione penale come un *continuum*» rispetto alla fase di pre-inchiesta.

[192] In tal senso, ancora, F. DE LEO, *Il pubblico ministero*, cit., p. 1442, secondo cui l'attività di informazione «non può essere praticata, e neppure concepita, in compartimento distinti, ma costituisce un unico serbatoio a cui tutte le polizie attingono in funzione di una comune attività investigativa».

[193] L. D'AMBROSIO, *La pratica di polizia giudiziaria*, vol. I, Milano, 2007, p. 230.

[194] R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, cit., p. 136, il quale sottolinea come vi sia il rischio che le operazioni investigative realizzate su materiale informatico possano facilmente degenerare in strumenti «di ricerca di altre, nuove notizie di reato». Negli stessi termini, più di recente, v. P.P. PAULESU, *Notizia di reato e scenari investigativi complessi*, cit., p. 802; A. CAMON, *La fase che "non conta e non pesa": indagini governate dalla legge*, in AA.VV., *Legge e potere nel processo penale*, Milano, 2017, p. 112; M. PITTIRUTI, Digital evidence *e procedimento penale*, Torino, 2017, p. 143.

[195] R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, cit., p. 136. Analogamente, v. P.P. PAULESU, *Notizia di reato e scenari investigativi complessi*, cit., p. 802; A. CAMON, *La fase che "non conta e non pesa"*, cit., p. 112.

dell'azione penale, rischia di provocare un *vulnus* in termini di efficienza a causa dell'incapacità degli Uffici giudiziaria di smaltire un numero ingente di *notitie criminis*[196].

È innegabile, però, che occorra distinguere a seconda dell'operazione realizzata nel corso dell'inchiesta preparatoria. Nessuno dubita che la polizia amministrativa possa avvalersi di *software* di *cyberpatrolling* per raccogliere informazioni, ad esempio, su determinati contesti criminosi, anche prima dell'avvio formale di un'indagine. Ben diverso, però, è il caso (che qui si analizza) in cui la medesima operazione sia compiuta in maniera non occasionale, bensì sistematica: in tale evenienza, per riprendere le parole di autorevole dottrina, «quella stessa attività preventiva si salda funzionalmente all'attività repressiva mutando così la propria natura»[197].

È in questa prospettiva, allora, che occorre chiedersi se il *cyberpatrolling* continuativo e individualizzato possa essere esperibile nell'ambito delle investigazioni pre-procedimentali.

Da tempo in letteratura ci si interroga sui limiti spaziali e temporali che dovrebbero caratterizzare questa fase. Del resto, la necessità di approntare meccanismi di tutela a favore dell'interessato in tale contesto era già emersa agli inizi degli anni '80, quando la Corte costituzionale ebbe a disconoscere espressamente quell'orientamento pretorio volto a negare ogni forma di garanzia nello svolgimento di attività di controllo *extra* procedimentale alla luce della loro natura squisitamente amministrativa. In quell'occasione, i giudici di Palazzo della Consulta, con una pronuncia «marcatamente innovativa»[198], affermarono che il diritto di difesa sarebbe violato «qualora la nozione di procedimento, nel quale il comma 2 dell'art. 24 Cost. garantisce la difesa come diritto inviolabile, venisse intesa in senso restrittivo, escludendo le attività preordinate a una pronuncia penale»[199].

Ebbene, in tale contesto la dottrina sostiene generalmente che nel corso della fase diretta all'acquisizione della notizia di reato debbono ritenersi consentiti tutti quegli atti tipici o atipici che non incidono sui diritti costituzionalmente garantiti agli artt. 13 ss. Cost., per la limitazione dei quali il legislatore costituzionale richiede l'osservanza della riserva di legge e della riserva di giurisdizione[200]. Di conseguenza, non sono considerate ammissibili, prima di una formale iscrizione *ex* art. 335 c.p.p., le ispezioni, le perquisizioni, i sequestri e le intercettazioni. Al contrario, possono contemplarsi tutti gli atti investigativi che non implicano l'esercizio di un potere statale autoritativo, quali l'assunzione di sommarie informazioni, i sopralluoghi, i rilievi fotografici, l'acquisizione di documenti e i pedinamenti.

---

[196] Mette in luce questo aspetto, P.P. PAULESU, *Notizia di reato e scenari investigativi complessi*, cit., p. 802.

[197] R. ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata*, cit., p. 583, nt. 47.

[198] Così, a commento di Corte cost., 15 luglio 1983, n. 248, M. NOBILI, *Atti di polizia amministrativa utilizzabili nel processo penale e diritto di difesa: una pronuncia marcatamente innovativa*, in *Foro it.*, 1984, I, p. 375 ss.

[199] Corte cost., 15 luglio 1983, n. 248, cit.

[200] La tesi è senza alcun dubbio dominante in letteratura. Cfr., ad es., A. ZAPPULLA, *La formazione della notizia di reato*, cit., p. 264-274; R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, Napoli, 2010, p. 50-52; A. MARANDOLA, *I registri del pubblico ministero tra notizia di reato ed effetti procedimentali*, Padova, 2001, p. 113-120; P. FERRUA, *L'iniziativa del pubblico ministero nella ricerca della* notitia criminis, in *Leg. pen.*, 1986, p. 317, che esclude tanto gli «atti coercitivi» tanto gli «atti di carattere probatorio». L'orientamento è condiviso dalla giurisprudenza di legittimità: cfr., per tutte, Cass. pen., Sez. I, 17 aprile 2012, n. 14484.

Alla luce di queste coordinate teoriche, si dovrebbe affermare che il *social network monitoring* vada ricompreso in quest'ultima categoria, posto che non pare trattarsi di attività limitativa dei diritti fondamentali sanciti agli artt. 13 ss. Cost.

Ciò nondimeno, è forse possibile provare a impostare la questione in termini differenti.

L'interpretazione tradizionale in base alla quale gli atti realizzabili nella pre-inchiesta sarebbero solo ed esclusivamente quelli che non arrecano un *vulnus* alle libertà *ex* art. 13 ss. Cost. appare «riduttiva e formalistica»[201], perlomeno in un'epoca nella quale si assiste quasi quotidianamente alla nascita di "nuovi diritti"[202] volti a tutelare l'individuo dalle intrusioni nella sfera privata causate dall'impiego di strumenti di indagine digitale altamente invasivi. Tra questi, non v'è dubbio che la *privacy* costituisca una prerogativa meritevole di tutela anche in sede pre-procedimentale, specie laddove l'autorità investigativa realizzi attività di *cyberpatrolling* individualizzato in maniera costante e continuativa. A sostengo di questa conclusione risulta utile richiamare un passaggio di una risalente – ma quantomai attuale – pronuncia della Suprema Corte[203], nella parte in cui si afferma che l'art. 330 c.p.p. costituisce una «norma di sbarramento» a tutela delle libertà del singolo cittadino, poiché inibisce all'autorità pubblica di adottare provvedimenti che incidono negativamente sui diritti fondamentali. Tra questi, come detto, non può che essere ricompresa anche la riservatezza.

Ad abundantiam, non appare fuor d'opera osservare come la dottrina, del resto, abbia escluso la possibilità di realizzare un pedinamento elettronico tramite GPS nel corso della pre-inchiesta proprio in quanto quest'ultimo si risolverebbe in un'intollerabile violazione della *privacy*, «risultando infatti compressi sia il diritto al riserbo sulle vicende personali sia la facoltà individuale di "autodeterminazione informativa" quanto ai propri dati»[204]. Laddove si condivida questa esegesi[205] e si consideri che l'attività di *cyberpatrolling* risulta certamente più invasiva – per le ragioni sopra ricordate – rispetto a un pedinamento tradizionale[206] o un pedinamento GPS[207], deve concludersi, *a fortiori*, a favore di un divieto di utilizzo della sorveglianza individualizzata nei *social network* nel corso delle investigazioni per la notizia di reato. Diversamente opinando, sarebbe «vanificato lo sforzo del legislatore del 1988 di esorcizzare il rischio del possibile riproporsi di istruzioni di p.g. libere, capillari, scevre da vincoli formali»[208], così come avvenuto nella vigenza del codice del '30.

---

[201] Così la definisce D. CURTOTTI, *"Le operazioni digitali sotto copertura"*, cit., p. 517.

[202] Cfr., Parte II, Cap. I.

[203] Cass. pen., Sez. III, 26 gennaio 1999, in *Cass. pen.*, 1999, p. 3458.

[204] La tesi è sostenuta, ad es., da C. FANUELE, *La localizzazione* satellitare, cit., p. 51, da cui è tratta la citazione.

[205] *Contra*, A. ZAPPULLA, *La formazione della notizia di reato*, cit., p. 278 s., il quale argomenta facendo leva proprio sulla compatibilità del pedinamento GPS con le libertà sancite agli artt. 13 ss. Cost.

[206] La conclusione, a ben vedere, non è destinata a mutare neppure laddove l'attività sia svolta "a catena", ovverosia da parte di più agenti di polizia.

[207] Concorde R. LEVINSON-WALDMAN, *Private Eyes, Thery're Watching You: Law Enforcement's Monitoring of Social Media*, in *Oklahoma Law Review*, 2019, p. 1010.

[208] D. CURTOTTI, *"Le operazioni digitali sotto copertura"*, cit., p. 517

6.2 Le *open source information* ricavate dai *social network* tra attività di *predictive policing* e tecnologie di riconoscimento facciale

Come si è osservato, l'attività di *social network mining* consente alle forze di sicurezza di creare veri e propri "schedari digitali" contenenti informazioni aventi natura più disparata. Alla luce di ciò, non deve stupire che l'autorità pubblica abbia colto fin da subito le grandi potenzialità legate all'impiego dell'intelligenza artificiale proprio "in combinato congiunto" con i predetti *software* di *cyberpatrolling*[209].

In una prospettiva ancora generale, i più accreditati studiosi hanno sottolineato come duplici siano gli ambiti processuali nei quali l'impiego di dispositivi basati sull'IA si è fatto particolarmente pervasivo e, allo stesso tempo, problematico[210] .

Il riferimento corre, *in primis*, ai cd. algoritmi predittivi, una categoria all'interno della quale è possibile distinguere i *software* di *predictive policing* da altri apparati informatici in grado di realizzare attività predittive su comportamenti futuri. I primi, come noto, consentono, attraverso l'incrocio di dati provenienti da fonti eterogenee, di prevedere i luoghi di probabile, futura commissione di reati (cd. *place-based system*) o di individuare i profili dei possibili autori di condotte illecite (*person-based system*)[211]. Si tratta di un nuovo paradigma di *crime managment* che, a differenza di un approccio esclusivamente reattivo al fenomeno criminale (si legga, *post-delictum*), si pone quale obiettivo quello di realizzare misure di sicurezza pubblica atte a prevenire la realizzazione di attività *contra legem*[212]. Nella seconda classe, invece, possono essere annoverati i *risk assessments tools*, ossia strumenti fondati sull'IA e impiegati, per lo più, nel corso del procedimento penale (e, in specie, in fase cautelare) «in grado di calcolare il rischio che un prevenuto si sottragga al processo o commetta dei reati»[213].

L'altro terreno d'elezione è quello relativo alle tecnologie biometriche, ovverosia strumentazioni in grado di analizzare e "matchare" in maniera automatizzata caratteristiche

---

[209] La letteratura relativa al rapporto tra rito e IA, limitatamente al panorama italiano, è già divenuta "tsunamica". Consci del rischio che potrebbe derivare da un richiamo probabilmente arbitrario, si rinvia alla raccolta recentemente e autorevolmente predisposta da M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 52, nt. 6.

[210] Si vedano J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, p. 1059 s.; M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Dir. pen. cont.*, 29 maggio 2019, p. 2 s.; G. LASAGNI, *AI-Powered Investigations: From Data Analysis to an Automated Approach Toward Investigative Uncertainty*, in L. Bachmaier Winter – S. Ruggeri (a cura di), *Investigating and Preventing Crime in the Digital Era. New Safeguards, New Rights*, Cham, 2022, p. 169 ss.; S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020, *passim*; S. SIGNORATO, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. proc.*, 2020, p. 605 ss.

[211] In termini generali, dunque, si può affermare che le diverse applicazioni in uso alla polizia consento di realizzare attività predittive sia con riguardo ai luoghi, sia con riguardo agli individui. Cfr. S. LONATI, Predictive policing*: dal disincanto all'urgenza di un ripensamento*, in *Rivista diritto dei media*, 2022, 2, p. 302.

[212] A.G. FERGUSON, *Policing Predictive Policing*, in *Washington Law Review*, 2017, p. 1137; M. CAIANIELLO, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventinve Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2021, 29, p. 10.

[213] M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 3.

anatomiche o fisiologiche di una persona. Il riconoscimento facciale, da questo punto di vista, rappresenta, senza ombra di dubbio, una delle più discusse e, al contempo, efficaci tecniche investigativo-probatorie: rispetto ad altre metodologie di analisi biometriche, infatti, essa presenta il vantaggio di non essere invasiva, non richiedendo alcuna collaborazione attiva del bersaglio[214].

Da questa prospettiva, ciò che qui preme sottolineare è lo stretto legame che intercorre tra questi nuovi approcci investigativi fondati sull'intelligenza artificiale e le informazioni *open access* presenti nelle piattaforme di *sharing*: esse rappresentano una fonte preziosa – e, verrebbe da dire, tra le più significative (qualitativamente e quantitativamente parlando) – sia per lo svolgimento di attività di polizia predittiva, sia per l'implementazione delle *automated facial recognition technologies*.

Sul primo fronte, si è assistito, negli ultimi anni, a una crescita esponenziale dell'impiego di informazioni pubblicamente disponibili nei *social network* per lo svolgimento di analisi predittive volte a prevenire la possibile commissione di attività delittuose. D'altro canto, se dette operazioni sono comunemente definite come lo studio e l'analisi di "dati" al fine di scongiurare il verificarsi di reati, non deve sorprendere che la maggior parte di essi siano estratti proprio dalle moderne piattaforme digitali[215], le quali, difatti, rappresentano la più grande banca "dati" attualmente disponibile. Le ricerche più accreditate[216], del resto, mostrano come l'analisi linguistica dei contenuti pubblicati in Rete migliori le prestazioni dei modelli di previsione del crimine rispetto all'impiego di informazioni tradizionali, cioè, reperite dalle autorità di *law enforcement* nel mondo analogico.

I dati diffusi pubblicamente in *Internet*, dunque, rappresentano una delle principali fonti archiviate dalle forze dell'ordine (mediante tecniche di *cyberpatrolling*) e in seguito utilizzate quali *input* per il funzionamento di *software* in grado di elaborare modelli predittivi[217]. La predilezione per questa *species* di patrimonio informativo è dovuta, in gran parte, alla sua gratuità e facile reperibilità; caratteristiche che inducono le autorità di pubblica sicurezza a farne un utilizzo smodato e senza alcuna restrizione.

Non si vuole certamente negare, è opportuno precisarlo, che nell'attuale contesto storico debba essere promossa l'idea di un rafforzamento dei meccanismi di prevenzione, anziché limitarsi a implementare misure *ex post*, destinate a produrre effetto una volta che la lesione al bene giuridico si è già realizzata. Ciò nondimeno, un problema di non poco conto con il

---

[214] E. SACCHETTO, Face to face: *il complesso rapporto tra* automated facial recognition technology *e processo penale*, in *Leg. pen.* web, 16 ottobre 2020, p. 2.

[215] La circostanza è sottolineata pure da G.M. BACCARI – C. CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in *Dir. pen. proc.*, 2021, p. 711 ss.

[216] Tra i primi studi tecnico-informatici sul punto, v. M.S. GEBER, *Predicting Crime using Twitter and kernel density estimation*, in *Decision Support Systems*, 2014, p. 115 ss.

[217] Con specifico riguardo alle tecniche di *data mining* per finalità di prevenzione dei reati, v. S. SIGNORATO, *Giustizia penale e intelligenza artificiale*, cit., p. 607-609. Un *software* sviluppato oltreoceano, denominato *Beware*, ad esempio, utilizza dati ricavati in prevalenza dai *social network* per individuare dove e quando potrebbero essere realizzate attività illecite (*https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html*). Si pensi, altresì, nel panorama nazionale, al *software* XLAW, sperimentato in alcune città italiane a partire dal 2013, il cui funzionamento si basa proprio un algoritmo in grado di elaborare una mole enorme di dati estrapolati anche dalle piattaforme di *sharing*.

quale, nel solco dell'analisi che si va conducendo, occorre confrontarsi riguarda la fase di raccolta dei dati inseriti in *input*, in seguito utilizzati dall'algoritmo per emettere la sua "decisione"[218]. Detta operazione, infatti, non sembra conformarsi ai crismi di legalità indicati all'art. 8 CEDU e, più in generale, all'idea di *privacy in the public space*, così come enucleata dalle Corti europee[219]. Mette conto ricordare, in proposito, che il rispetto dei diritti fondamentali rappresenta uno dei principi chiave nel contesto dell'implementazione di qualunque sistema di intelligenza artificiale. L'assunto è stato espresso a chiare lettere nella *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale*, ove si individua quale primo pilastro di qualsivoglia regolamentazione in materia proprio la necessità di assicurare che l'elaborazione e l'attuazione di strumenti e servizi di IA siano compatibili con le libertà fondamentali degli individui[220].

Ebbene, in un recente studio del 2020 volto a mappare i possibili rischi legati all'impego delle nuove tecnologie nel campo delle operazioni di *law enforcement* e della giustizia penale *lato sensu* intesa, si è sottolineato come la tutela della *privacy* rappresenti un valore irrinunciabile in una società democratica. Più in particolare, il *report* ha messo in luce come non dovrebbero tollerarsi interferenze nella sfera di riservatezza dei singoli cittadini pure laddove gli strumenti di polizia predittiva operino grazie a una raccolta massiva di informazioni *open source*[221].

Le potenzialità collegate all'analisi massiva delle informazioni *open access* per finalità di prevenzione dei reati, lo si è accennato, non riguardano solamente le attività di *predictive policing*.

Onde avere un concreto esempio di ciò, è sufficiente menzionare lo scandalo *Clearview* che, come risaputo, ha avuto un forte impatto non solo oltreoceano, ma anche nel vecchio continente[222]. Società con sede legale negli Stati Uniti e operante nel settore delle *Information Technogies*, la *start-up* newyorkese fondata nel 2017 commercializzava (e commercializza tutt'ora) un *software* di riconoscimento facciale in grado di supportare l'attività delle agenzie americane (ed europee) che svolgono funzioni di *law enforcement* e di repressione criminale. A seguito di uno *scoop* giornalistico apparso nel *New York Times*

[218] Un'ulteriore tematica – che esula, però, dalla presente trattazione – è quella relativa alla qualità dei dati raccolti, cui si legano le problematiche sul versante del potenziale impatto discriminatorio degli algoritmi. Cfr., per tutti, S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020, *passim*.

[219] Cfr. *infra*.

[220] COMMISSIONE EUROPEA PER L'EFFICIENZA E LA GIUSTIZIA, *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale*, 3 dicembre 2018, p. 10. Sulla necessità che le operazioni di trattamento automatizzato e "intelligente" dei dati siano realizzate conformandosi ai principi che reggono l'ordinamento giuridico, v. M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 56, ove si richiama, in senso adesivo, il *dictum* di una tra le prime pronunce del giudice amministrativo in materia (Cons. Stato, 13 dicembre 2019, n. 8472).

[221] POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS – EUROPEAN PARLAMENT, *Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights*, luglio 2020, p. 40.

[222] Sul punto, v. J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 1069; M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 54; e, per un'approfondita disamina del caso, I. NERONI REZENDE, *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, in *New Journal of European Criminal Law*, 2020, p. 375 ss.

agli inizi del 2020[223], si è appreso con stupore che la società aveva raccolto da *Facebook*, *YouTube* e altri *social network* oltre tre miliardi di immagini pubblicamente disponibili, raffiguranti i volti di milioni di utenti. Una volta eseguita tale operazione di *data scraping*, le raffigurazioni così ottenute venivano catalogate all'interno di un *database* privato, in seguito offerto alle forze dell'ordine per identificare gli autori di atti illeciti. Clearview AI, difatti, consentiva (e consente ancora oggi) di individuare una corrispondenza tra l'immagine in possesso delle autorità e quella eventualmente presente nella banca dati.

L'attività di *screening* realizzata dalla compagnia statunitense, pur collocandosi nel solco di quella generale (e, per certi versi, auspicata) cooperazione pubblico-privata che dovrebbe caratterizzare le attività investigative *on the web*[224], differisce in gran parte dalle classiche forme di collaborazione tra *provider* e autorità statali. Si allude, più in particolare, al fatto che la raccolta massiva di informazioni viene realizzata da un soggetto privato in spregio delle più elementari garanzie a salvaguardia della *privacy*; garanzie che, lo si è detto a più riprese, debbono trovare applicazione pure in contesti *open access*. Sembra così profilarsi all'orizzonte uno scenario – tutt'altro che rassicurante – nel quale le autorità pubbliche fanno uso di dati acquisiti *online* da soggetti terzi in violazione delle libertà fondamentali, eludendo in tal modo i limiti e le tutele approntate dalle norme convenzionali (in specie, gli artt. 7 e 8 della Carta di Nizza e l'art. 8 CEDU)[225]. In assenza di un consenso esplicito manifestato dagli interessati – requisito legato inscindibilmente a quel più generale «*right to control the use of image*», enucleato dalla Corte di Strasburgo[226] – e in mancanza di un'autorizzazione *ad hoc* dei gestori delle piattaforme[227], Clearview AI procede a un trattamento massiccio e indiscriminato (*rectius*, raccolta e strutturazione) di immagini ricavate dai *social network*.

In realtà, a sostegno della legittimità (e liceità) di detta operazione, si potrebbe invocare, a prima vista, il dettato dell'art. 9, comma 2, lett. e) del GDPR[228], a mente del quale è consentito, in deroga al divieto generale previsto al primo comma, il trattamento di «dati biometrici» intesi a identificare in modo univoco una persona fisica, qualora essi siano stati «resi manifestamente pubblici dall'interessato». Lo stesso art. 10, comma 1, lett. c) della Direttiva 2016/680/UE, relativa al trattamento dei dati personali da parte delle autorità pubbliche a fini di prevenzione e repressione dei reati, del resto, consente, in termini non dissimili, la raccolta e l'elaborazione dei dati biometrici «*manifestly made public by the data subject*». Un principio, quest'ultimo, pedissequamente recepito dal legislatore nazionale all'art. 7 del d.lgs. 51/2018[229]. Nessun dubbio, del resto, circa la riconducibilità dei contenuti visivi *open access* elaborati dalla piattaforma Clearview IA nella categoria dei «dati

[223] *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html*.

[224] Cfr. Parte II, Cap. V, par. 8.

[225] Come sottolineato da J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 1069, «applicando *tool* di riconoscimento facciale […] alle immagini reperibili sul *web*, diventa possibile controllare, in modo capillare, la nostra vita privata».

[226] Corte edu, 11 giugno 2020, *P.N. c. Germania*, par. 56.

[227] I *Social network provider*, per tale ragione, hanno promosso numerose cause legali nei confronti dell'azienda americana, con l'obiettivo di ottenere l'interruzione di queste pratiche di rastrellamento dei dati (*https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/*).

[228] *General Data Protection Regulation*, adottato il 27 aprile 2016.

[229] D.lgs. 18 maggio 2018, n. 51.

biometrici», giacché trattasi di informazioni ottenute da un trattamento tecnico specifico che consente l'identificazione univoca di un determinato soggetto[230]. A conferma di ciò, soccorre quanto osservato dal Working party 29 che, nell'esaminare alcuni aspetti fondamentali della Direttiva 2016/680/UE, ha sottolineato come la natura *open* dei dati debba essere riconosciuta tutte le volte in cui la persona interessata sia consapevole della loro diffusione "al pubblico"[231].

Ciò nondimeno, queste forme di *bulk data scraping* debbono ritenersi, *de lege* (non) *lata*, incompatibili con il diritto alla riservatezza; una prerogativa che, lo si è detto a più riprese, trova pieno riconoscimento pure con riguardo alle informazioni liberamente accessibili da chiunque. Allo stato attuale, difatti, qualunque forma di acquisizione massiva di dati biometrici ricavati dai *social network* non può dirsi conforme ai requisiti di stretta necessità e proporzionalità fissati dalla normativa europea e nazionale (GDPR, Direttiva 2016/680/UE; d.lgs. 51/2018). In effetti, un conto è autorizzare le autorità di pubblica sicurezza e di repressione criminale alla raccolta e all'impiego, per finalità *lato sensu* investigative, di determinati dati *open access*. Ben altro è consentire loro di usufruire di "contenuti visivi" riferibili a soggetti neppure coinvolti in situazioni potenzialmente attenzionabili dall'autorità statale e ottenuti a seguito di una raccolta massiva, indiscriminata e *sine tituto*[232]. Prova ne sia quanto previsto nel provvedimento adottato dall'*European Data Protection Board* relativo all'utilizzo delle tecnologie di riconoscimento facciale nel territorio dell'Unione europea[233]. A tal proposito, è dato leggere, a chiare lettere, che l'impiego di immagini o fotografie digitali caricate dagli utenti nei *social network* non può essere considerato legittimo sulla sola base del fatto che dette informazioni sono state rese manifestamente pubbliche dagli interessati[234].

Alle medesime conclusioni, peraltro, sono giunti pure i giudici europei. Nella recente pronuncia *Glukhin c. Russia*[235], la Corte di Strasburgo ha riscontrato la violazione degli artt. 8 e 10 della Carta in un caso nel quale il ricorrente, identificato dalle forze dell'ordine grazie a sistemi di riconoscimento facciale che utilizzavano immagini ricavate dai canali *Telegram* e da altre pagine *social*, era stato condannato in via amministrativa per aver omesso di notificare alle autorità la sua intenzione di organizzare una manifestazione pubblica. A sostengo delle proprie argomentazioni, i giudici sovranazionali hanno valorizzato proprio quella "componente esterna" dell'art. 8 CEDU qualificata in termini di «*private social life*», ovverosia «*the possibility of stablishing and developing relationships with others and the*

[230] È questa la definizione offerta dall'art. 4, comma 1, n. 14) del GDPR, dall'art. 3, comma 1, n. 13) della Direttiva 2016/680/UE, nonché dall'art. 2, comma 1, lett. o) del. D.lgs. n. 51/2018. In questo senso, v. pure I. NERONI REZENDE, *Facial recognition in police hands*, cit., p. 382.

[231] WORKING PARTY 29, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*, 29 novembre 2017, p. 10.

[232] Concorde pure D. BOYD, *Privacy and Publicity in the Context of Big Data*, 29 aprile 2010, al sito *https://www.danah.org/papers/talks/2010/WWW2010.html*.

[233] EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 26 aprile 2023.

[234] EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, cit., par. 107.

[235] Corte edu, 14 luglio 2023, *Glukhin c. Russia*.

outside world»[236]. Una prerogativa che sarebbe violata nel caso in cui la legislazione di uno Stato membro consentisse alle forze di sicurezza di impiegare liberamente e senza limiti dati personali pubblicamente accessibili.

Alla luce di quanto osservato, non può che condividersi la scelta del Parlamento europeo di approvare, in data 14 giugno 2023, un emendamento alla Proposta di Regolamento sull'IA (*Artificial Intelligence Act*)[237], approvata in data 13 marzo 2024, volto a limitare le attività di *data scraping*. Ad integrazione del considerando n. 26 della suddetta Proposta, il legislatore comunitario ha stabilito il divieto, assoluto e inderogabile, di ricorrere a strumenti informatici in grado di estrarre indiscriminatamente e in maniera "non mirata" «*biometric data from social media*» per creare o ampliare *database* di riconoscimento facciale. Trattasi, ad avviso del Parlamento, di operazioni che contribuiscono a generare «*the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy*». La modifica apportata rappresenta un'ulteriore conferma dell'idea secondo cui la natura pubblica dei contenuti diffusi, pur volontariamente, in Rete non autorizza un loro trattamento massivo, neppure per finalità di prevenzione dei reati, perdipiù in assenza di un'idonea base legale.

7. *Social network mining* e indagini preliminari

Ben potrebbe accadere che nel corso delle indagini preliminari (si legga, dopo l'iscrizione della notizia di reato) la polizia giudiziaria, nell'esercizio della propria funzione di repressione criminale, abbia la necessità di apprendere informazioni pubblicamente disponibili nei *social network*. Trattasi, a dispetto di quanto si possa pensare, di un'operazione sempre più frequente nella prassi investigativa[238]. Onde rendersi conto di ciò, è sufficiente segnalare come uno studio condotto nell'ambito della piattaforma *LexisNexis* abbia evidenziato che circa l'80% delle forze dell'ordine eseguono quotidianamente ricerche all'interno delle piattaforme digitali, al fine di reperire materiale utile alla prosecuzione delle indagini[239]. Del resto, gli analisti più attenti hanno sottolineato come le *social webpages*

---

[236] Corte edu, 14 luglio 2023, *Glukhin c. Russia*, cit., par. 64.

[237] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, 21 aprile 2021 (*https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.pdf*).

[238] Ne dà conto, richiamando esperienze sviluppatesi in numerosi ordinamenti europei, S. BARRERA, *Claves de la Investigaciòn en Redes Sociales*, cit., p. 237. Nella dottrina italiana, ha messo recentemente in luce questo aspetto pure M. TORRE, Open source intelligence: *spionaggio digitale e* social network, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 1710, per il quale detta modalità di ricerca della prova rappresenta «una fonte di informazioni spesso insostituibile per l'inizio e la prosecuzione delle indagini relative a sempre maggiori forme di criminalità».

[239] Per tale ragione, la compagnia ha sviluppato un sistema chiamato *Social Media Monitor* che consente agli agenti di polizia di monitorare tutti i canali di *social media* di uno specifico soggetto. Si tratta, in realtà, di uno tra i numerosi *software* a disposizione delle autorità investigative di tutto il mondo (*https://risk.lexisnexis.com/insights-resources/infographic/law-enforcement-usage-of-social-media-for-investigations-infographic*). In questo senso, il *Police Executive Research Forum* ha messo in luce come l'86% degli agenti di polizia intervistati abbia dichiarato di monitorare i *social network* per identificare piste investigative (J. BYRNE – G. MARX, *Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact*, in *Journal of Police Studies*, 2011, p. 27). Anche ulteriori sondaggi hanno rilevato come l'80% delle autorità di *law enforcement* «*used social media platforms as intelligence gathering tools*». (*https://strongvisa.com/wp-content/uploads/2011/07/Social_Media_Surveillance_and_Law_Enforcement-2015.pdf*).

siano considerate dagli inquirenti uno strumento prezioso, poiché consentono di «vedere e monitorare attivamente e costantemente le attività di un sospettato o di un bersaglio […] mantenendo allo stesso tempo un alto livello di anonimato»[240].

In tale contesto, non deve stupire se alcuni ordinamenti – si pensi, ad esempio, a quello olandese – hanno già istituito, presso ogni Dipartimento di polizia giudiziaria, gruppi di investigazione specificatamente dedicati alla ricerca di dati pubblicamente disponibili nella Rete; un'attività di profilazione, quest'ultima, che – come sottolineato dalle stesse autorità di polizia – viene svolta in modo rutinario con riferimento ai profili *social* in uso all'indagato[241].

A ragione, pertanto, l'operazione *de qua agitur*, nuova frontiera nell'ambito delle indagini penali *stricto sensu* intese[242], può essere annoverata, senza troppe difficoltà, nel più ampio compendio delle moderne misure investigative che sfruttano sistemi tecnologicamente avanzati di controllo occulto. Per tale motivo, e al fine di comprendere nel dettaglio le problematiche poste sul versante nazionale dall'impiego di questa tecnica, è utile operare un richiamo cursorio alle discipline giuridiche di quegli ordinamenti stranieri che hanno implementato forme di *online surveillance* procedimentale, ancorché non limitate all'apprensione di fonti aperte.

La legge penalprocessuale olandese, ad esempio, regolamenta espressamente l'ipotesi in cui la polizia giudiziaria esegua un'attività di *systematic surveillance*, anche mediante l'impiego di strumentazioni digitali. La sezione 126g del codice di rito, più nel dettaglio, stabilisce che il pubblico ministero può autorizzare le forze dell'ordine a seguire od osservare sistematicamente gli spostamenti di una persona. Si prevede, inoltre, che il «mandato di sorveglianza» debba essere redatto per iscritto[243], indicando la durata del monitoraggio (massimo tre mesi), il tipo di reato per il quale si procede e le concrete modalità esecutive[244].

Anche l'ordinamento tedesco ha adottato una regolamentazione *ad hoc*, operando una distinzione tra attività di *surveillance* realizzate in modalità presenziale (art. 163f StPO) e operazioni di vigilanza che richiedono l'impiego di strumentazioni tecnologiche (100h StPO). In generale, la legge attribuisce esclusivamente al giudice[245] il potere di emettere un «ordine di osservazione a lungo termine», cioè per un periodo ininterrotto superiore alle 24 ore o che si protrae per più di due giorni. Tra i presupposti dell'attività di sorveglianza, il

---

[240] J. BRUNTY – K. HELENEK, *Social Media Investigation for Law Enforcement*, New York, 2013, p. 55 (trad. nostra).

[241] Il dato è riportato da S. BARRERA, *Claves de la Investigaciòn en Redes Sociales*, cit., p. 83.

[242] Lo affermano espressamente J.P. MURPHIY – A. FONTECILLA, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, in *Richmond Journal of Law & Technologiy*, 2013, p. 11. Lo sottolinea, ancorché incidentalmente, pure F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., p. 101.

[243] Il comma 6 dello stesso articolo, in realtà, prevede che in caso di necessità ed urgenza, il mandato può essere emesso verbalmente, salvo successiva convalida entro tre giorni.

[244] Per un approfondimento sulla disciplina olandese in materia, v. B.J. KOOPS, *Police Investigations in Internet Open Source*, cit., p. 654 ss., il quale ricorda come nel Paese sia attualmente in uso alla polizia un sistema di *social network monitoring*, denominato *iColumbo*, in grado di monitorare i profili pubblici per finalità preventivo-investigative (p. 655).

[245] In realtà, in circostanze di straordinaria eccezionalità ed urgenza, il pubblico ministero è legittimato a emettere d'iniziativa un ordine di sorveglianza, salvo convalida da parte del giudice entro tre giorni dall'adozione del provvedimento.

codice prevede la sussistenza di sufficienti indizi che dimostrino la commissione di un reato di notevole rilevanza, nonché, in ossequio al principio di sussidiarietà e necessarietà, che l'autorità investigativa non possa disporre di altri mezzi di accertamento in grado di raggiungere il medesimo risultato con minor sacrificio. Sul versante soggettivo, poi, la misura può avere quale bersaglio tanto l'indagato, quanto soggetti terzi; ma, in quest'ultimo caso, la limitazione della *privacy* può avvenire solo laddove si possa presumere, alla luce di elementi concreti, che questi abbiano un legame con l'autore del reato o che l'intromissione nella sfera di riservatezza risulti necessaria per l'accertamento dei fatti.

A fronte di tale (sintetico) affresco, la situazione italiana appare davvero poco rassicurante. Come si è già ricordato, infatti, l'attività di *social network mining* risulta del tutto priva di regolamentazione.

Un simile vuoto normativo non ha impedito, comunque, a quella (ancor minima) parte della dottrina che si è occupata del tema, di ricondurre l'operazione in questione nell'alveo di quelle attività atipiche di polizia giudiziaria disciplinate agli artt. 55, 348 e 370 c.p.p., per lo svolgimento delle quali, com'è noto, la legge non richiede un provvedimento autorizzativo dell'autorità procedente[246]. Ricorrendo a un'analogia tra mondo fisico e virtuale, si è sostenuto che l'attività di sorveglianza equivarrebbe agli appostamenti o ai pedinamenti tradizionalmente operati dalle forze dell'ordine, nelle more del procedimento, in luoghi liberamente accessibili al pubblico. Ciò che distinguerebbe le due attività, in sostanza, sarebbe esclusivamente il "luogo" nel quale esse vengono espletate: l'una, nelle strade delle città, l'altra, nel cyberspazio. Adottando questa prospettiva, perciò, si comprende come le operazioni di monitoraggio virtuale volte all'apprensione di contenuti liberamente accessibili a tutti gli utenti dei *social network* siano state annoverate tra le attività investigative innominate, al pari del pedinamento tradizionale[247] e del pedinamento elettronico tramite GPS[248]. Le conseguenze sul piano delle garanzie procedurali sono facilmente intuibili: trattandosi di un mezzo di ricerca della prova non disciplinato dalla legge e che non incide su beni di immediato rilievo costituzionale[249], il *cyberpatrolling* può essere eseguito d'iniziativa dagli organi di polizia pur in assenza di un'autorizzazione previa[250].

---

[246] Questa tesi è esplicitamente sostenuta da A. APRUZZESE, *La recente normativa in tema di contrasto del terrorismo*, cit., p. 234; C. CONTI – M. TORRE, *Spionaggio digitale nell'ambito dei* social network, cit., p. 550, ove detta attività viene qualificata come una forma 2.0 di «pedinamento virtuale»; M. TORRE, Open source intelligence: *spionaggio digitale e* social network, cit., p. 1712, 1715; ID., Privacy *e indagini penali*, Milano, 2020, p. 136.

[247] Cass. pen., Sez. VI, 3 giugno 1998, n. 2072, in *Cass. pen*., 2000, p. 689; Cass. pen., Sez. V, 27 febbraio 2002, cit.; Cass. pen., Sez. II, 30 ottobre 2008, n. 44912.

[248] Cfr. Cass. Pen., Sez. II, 4 aprile 2019, n. 23172; Cass. pen., Sez. VI, 11 dicembre 2017, n. 15396; Cass. pen., Sez. IV, 27 novembre 2013, n. 21644.

[249] In questi termini si esprime la giurisprudenza di legittimità per giustificare il compimento di quelle attività di «osservazione, controllo e pedinamento» svolte d'iniziativa dalla polizia giudiziaria. Trattasi – si sostiene – di operazioni che «che non sono intrusive nella sfera privata, perché non limitano […] diritti costituzionalmente garantiti e, in particolare, la libertà morale del controllato», così, Cass. pen., Sez. VI, 3 giugno 1998, n. 2072, cit.

[250] Parrebbe adottare questa prospettiva C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. proc*., 2018, p. 1212 s.

L'assunto, a ben vedere, si pone in linea di continuità con il risalente e costante orientamento della giurisprudenza di legittimità in tema di videoriprese investigative[251]. In quella sede, com'è noto, il Supremo consesso ha stabilito che il *videotape* – avente ad oggetto mere immagini – effettuato in luoghi pubblici costituisce un atto non ripetibile e deve essere inquadrato nell'ambito delle prove atipiche previste dall'art. 189 c.p.p. La condotta non comunicativa – nella prospettiva adottata dai giudici e condivisa da una parte della dottrina[252] –, può essere liberamente captata dalla polizia giudiziaria di propria iniziativa, e in assenza di un "nulla osta" dell'autorità giudiziaria, in quanto «la natura del luogo in cui si svolge la condotta implic[a] una implicita rinunzia alla riservatezza»[253].

Le argomentazioni delle quali si è dato conto – e le relative conclusioni –, tuttavia, appaio eccessivamente *tranchant* e, per di più, sembrano non pienamente confacenti alle specificità degli strumenti di sorveglianza digitale di cui si discute.

Richiamando la distinzione tra monitoraggio passivo e monitoraggio attivo[254], può affermarsi che l'attività di *cyberpatrolling* debba essere ricompresa nell'ambito della seconda categoria. Ci troviamo al cospetto, infatti, di un'operazione soggettivamente canalizzata all'ottenimento di informazioni relative a uno specifico bersaglio, al fine di valutare la sua personalità, il suo comportamento (passato, presente e futuro), nonché a carpire le sue relazioni sociali.

Nello specifico, la vigilanza può essere condotta con due differenti modalità. In effetti, nel contesto del *social network monitoring*, come già osservato, appare doveroso distinguere tra un controllo *una tantum* e un monitoraggio continuativo.

Nel primo caso, la polizia giudiziaria si limita a osservare ed estrarre sporadicamente una o più informazioni dai profili *social* riconducibili a un determinato utente. Nessun dubbio che, in tale evenienza, gli inquirenti possano legittimamente visualizzare, apprendere e successivamente trattare l'informazione (sia essa un video, un'immagine, una dichiarazione etc.), pur in mancanza di un *placet* preventivo (giudiziario o giurisdizionale). Trattasi, infatti, di dati liberamente accessibili a chiunque, rispetto ai quali il singolo utente non può vantare alcuna aspettativa di riservatezza, giacché le informazioni sono state volontariamente e indiscriminatamente condivise con terzi[255].

---

[251] E, difatti, argomenta richiamando proprio il *dictum* della Corte, tra i fautori della tesi in esame, M. TORRE, Open source intelligence: *spionaggio digitale e* social network, cit., p. 1715.

[252] C. CONTI, *Il principio di non sostituibilità: il sistema probatorio tra Costituzione e legge ordinaria*, in *Cass. pen.*, 2024, p. 459, la quale riconduce detta casistica nelle ipotesi di «prove costituzionalmente indifferenti».

[253] Cass., Sez. Un., 28 luglio 2006, n. 26795. Sul tema, cfr. V. BONINI, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in *Proc. pen. giust*., 2019, p. 338 ss.; A. CAMON, *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. proc. pen*., 2006, p. 1550 ss.; C. CONTI, *Le videoriprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati"*, in *Dir. pen. proc.*, 2006, p. 1347 ss.; F. CAPRIOLI, *Riprese visive nel domicilio e intercettazione "per immagini"*, in *Giur. cost*., 2002, p. 2176 ss.

[254] Cfr. *supra*.

[255] Concordi, nella letteratura straniera, C.M. CORRELL, *Facebook, Crime Prevention, and the Scope of the Private Search Post-Carpenter*, in *Georgia Law Review*, 2022, p. 813; L.M. GLADYSZ, *Status Update*, cit., p. 713 s.; A.C. PAYNE, *Twitigation: Old Rules in a New Word*, in *Washburn Law Journal*, 2010, p. 860 s.

La conclusione, d'altro canto, è conforme all'interpretazione offerta dalla dottrina americana con riguardo all'estensione applicativa del IV emendamento, volto a tutelare la libertà dei cittadini a fronte di atti investigativi (*searches* e *seizures*) che non siano giustificati da un mandato giudiziario (*warrant*) supportato da una *probable cause*. In quel contesto, gli studiosi d'oltreoceano e le prime pronunce giurisprudenziali in argomento hanno ritenuto che le comunicazioni e le informazioni (anche di natura personale) condivise pubblicamente nei *social network*, in assenza di impostazione di *privacy* che ne limitino l'accessibilità, sono da considerarsi in "bella vista" e, pertanto, non possano giovarsi della protezione prevista dalla Carta Fondamentale. La logica sottesa è rintracciabile nella cd. *plain view doctrine* o *public disclosure doctrine* o, ancora, *public space doctrine* che, unitamente alla *Third Party Doctrine*[256], è volta a limitare lo spettro applicativo del IV emendamento a fronte di un comportamento attivo e volontario dell'individuo[257]. Stando a questa lettura, i cittadini non potrebbero invocare una ragionevole aspettativa di riservatezza tutte le volte in cui tengano volontariamente (*i*) un comportamento in pubblico (*ii*) suscettibile di essere osservato e monitorato da chiunque, incluse le autorità statali (*iii*). Di conseguenza, poiché l'utente non ha adottato precauzioni per proteggere la riservatezza dei propri dati, non può vantare alcuna aspettativa di *privacy*, né verso la collettività, né, tantomeno, nei confronti dell'autorità pubblica. Del resto, «*if you post a tweet, just like you scream it out the window, there is no reasonable expectation of privacy*»[258].

Simili argomenti, tuttavia, non sembrano altrettanto agevolmente spendibili nell'ipotesi di un controllo esercitato in modo continuativo.

Generalmente, il *quivis de populo* e, talvolta, le stesse autorità di polizia[259] hanno la percezione – facendo proprie le considerazioni poc'anzi svolte – che le informazioni liberamente accessibili contenute nei *social network* possano essere utilizzate da chiunque e per qualunque scopo, tanto dalle forze dell'ordine, quanto da privati cittadini, un po' come

[256] Ancorché la "dottrina della terza parte" e la "dottrina dello spazio pubblico" siano spesso esaminate congiuntamente, esse debbono essere tenute concettualmente distinte. La prima si riferisce all'ipotesi in cui un individuo riveli volontariamente informazioni a terzi. In questi casi, egli perde la protezione offerta dal IV emendamento, poiché si assume il rischio che la terza parte possa consegnarle all'autorità pubblica. Da questo punto di vista, la natura dell'informazione, pubblica o privata, è assolutamente irrilevante. Per converso, la *plain view doctrine* allude a quei casi nei quali un individuo che determinati comportamenti in ambienti pubblici che sono suscettibili di sorveglianza visiva ad opera delle forze dell'ordine. Cfr., per tutti, M. BEDI, *The Fourth Amendment Disclosure Doctrines*, in *William & Mary Bill of Rights Journal*, 2017, p. 461.

[257] La teoria è stata espressa per la prima volta nel caso *Katz c. Stati Uniti*, 389 U.S. 361 (1967), ove si affermò che oggetti, attività o affermazioni che un cittadino espone alla "semplice vista" degli estranei non sono protette dal IV emendamento, poiché non è stata mostrata alcuna intenzione di mantenerli segreti.

[258] *The People of the State of New York c. Harris*, 30 giugno 2012. Conformi, *ex plurimis*, *Stati Uniti c. Khan*, Case no. 15-cr-00286, 2017 WL 2362572 (N.D. Ill. 31 maggio 2017), par. 8, ove si afferma che l'imputato «*did not maintain any privacy restrictions on his Facebook account, and his Facebook profile was viewable by any Facebook user. Hence, defendant possessed no resonable privacy expectation in the information found on his Facebook page*»; *Stati Uniti c. Adkinson*, Case no. 4:15-cr-00025-TWP-VTW, 2017 WL 1318420 (S.D. Ind 7 aprile 2017), par. 5: «*there is no expectation of privacy in an open facebook page*». Concordi, in dottrina, E. NORTH, *Facebook Isn't Your Space Anymore*, cit., p. 1296; J.G. BROWNING, *Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, in *Science and Technology Law Review*, 2017, p. 485, ove si richiama una pronuncia del 2009 resa dalla Corte Suprema del Maryland nella quale si afferma che «*the act of posting information on a social networking sies, without the poster limiting access to that information, makes whatever is posted available to the world at large*».

[259] Ne danno ampiamente conto L. EDWARDS – L. URQUHART, *Privacy in Public Spaces*, cit., p. 14.

se il soggetto sottoposto a controllo stesse camminando per le strade di una città[260]. La pubblicazione di un post su *Facebook* – si sostiene – presuppone una rinuncia totale alla *privacy*, cosicché, i dati *open access*, fuoriuscendo dalla sfera di controllo dell'utente, divengono «*outlaw status and open all kinds of use*»[261]. D'altro canto – viene osservato – «*where someone does an act in public, the observance and recording of that act will ordinary not give rise to an expectation of privacy*»[262]. In altre parole, se un individuo sceglie volontariamente di rendere pubblico qualcosa sui *social network*, deve ritenersi che egli stia rinunciando implicitamente alla propria *privacy*. In quest'ottica, allora, si afferma che l'autorità statale (si legga, la polizia giudiziaria) possa legittimamente apprendere e conservare tutto ciò che viene pubblicato in Rete, senza la necessità di alcun provvedimento autorizzativo[263]. È chiaro il retropensiero: le informazioni diffuse in pubblico non risultano meritevoli di tutela costituzionale.

Questo *modus argomentandi*, tuttavia, non appare pienamente convincente, posto che finisce per considerare «la persona [digitale] come una miniera a cielo aperto dalla quale estrarre continuamente qualsiasi dato»[264]. Mutuando le parole utilizzate dal giudice Sotomayor nella nota *Concurring opinion* resa nel caso *Stati Uniti c. Jones*, nel contesto delle nuove forme di sorveglianza digitale eseguite mediante i *social network* occorre riconsiderare il tradizionale dogma secondo cui gli individui non avrebbero una ragionevole aspettativa di *privacy* con riguardo alle informazioni volontariamente divulgate a terzi. Un tale approccio «*is ill suited to the digital age*»[265].

In effetti, si è già sottolineato che l'aspettativa di riservatezza vantata dal cittadino (e dallo stesso indagato) sussiste anche nei luoghi esposti alla generale percezione visiva a fronte di

---

[260] In questi termini, v. D. LOSAVIO – M.M. LOSAVIO, *Prosecution and Social Media*, cit., p. 209.

[261] Così, E. DE BUSSER, *Open Source Data and Criminal Investigations*, cit., p. 113.

[262] In questi termini si esprime uno dei più accreditati esperti di criminalità informatica nel contesto britannico, A. GILLESPIE, *Regulation of Internet Surveillance*, in *European Human Rights Law Review*, 2009, p. 555. Nello stesso senso sembra collocarsi pure C. WARKEN, *Classification of Electronic Data for Criminal Law Purposes*, cit., p. 1.

[263] In termini espliciti, M. TORRE, Open source intelligence: *spionaggio digitale e* social network, cit., p. 1712. Mette conto osservare come questa idea risulti profondamente radicata anche nella letteratura straniera che si è occupata, ancorché incidentalmente, della tematica in esame. Si vedano, ad es., T. ARMENTA DEU, *Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre*, in *Revista de Internet, Derecho y Política*, 2018, 27, p. 75; P. ARRABAL PLATERO, *La prueba tecnològica: aportaciòn, pràctica y valoraciòn*, Valencia, 2020, p. 208; S. BARRERA, *Claves de la Investigaciòn en Redes Sociales*, cit., p. 237; F. BUENO DE MATA, *Investigación y prueba de delitos de odio en Redes Sociales*, cit., p. 154, 166 s.; D. LOSAVIO – M.M. LOSAVIO, *Prosecution and Social Media*, in C.D. Marcum – G.E. Higgins (a cura di), *Social Networking as a Criminal Enterprise*, Boca Raton, 2014, p. 209, per i quali «*openly accessible social media posting may be perused [by police] or other parties just as if they were walking down a street*»; N. PETRASHEK, *The Fourth Amendament and the Brave New World of Online Social Networking*, in *Marquette Law Review*, 2010, p. 1522; A. RODRÍGUEZ ÁLVAREZ, *Redes sociales y proceso penal: una radiografía*, in C. Alonso Salgado (a cura di), *El nuevo proceso penal sin Código Procesal Penal*, Barcellona, 2019, p. 331, la quale ritiene legittimo, in assenza di autorizzazione giudiziale, l'impiego del «*patrullaje virtual*», mediante l'utilizzo di «*programas* [*infomraticos*] *de búsqueda*», proprio perché riferito a dati e informazioni contenute in «*cuetas publicas*». L'assunto, come detto, è stato accolto anche dal Tribunale Supremo spagnolo sia con riguardo alla fase di prevenzione sia con riguardo a quella di repressione (investigativa *stricto sensu*) dei reati (cfr. *supra*).

[264] Si esprime in questi termini, nel criticare aspramente le moderne tecniche di *data mining* realizzate nelle piattaforme di *sharing*, S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, p. 322.

[265] *Stati Uniti c. Jones*, 565. 400 (2012).

attività dell'autorità giudiziaria volte a raccogliere, trattenere, ed esaminare sistematicamente le proprie informazioni[266]. Nessuno dubita – lo si è cercato di dimostrare *supra* – che un agente di polizia, al pari di un comune cittadino, possa apprendere e utilizzare per finalità investigative una notizia diffusa in pubblico[267]. Ben diverso, però, è il caso in cui quello stesso agente di polizia segua sistematicamente e in maniera occulta tutte le attività di vita quotidiana realizzate da un determinato individuo. Ciò che si intende sostenere, in altre parole, è che il profilo quantitativo e continuativo dell'attività di vigilanza finisce per incidere, inevitabilmente, sull'aspetto qualitativo della stessa, trasformandola in qualcosa d'altro rispetto alle tradizionali forme di "controllo analogico"[268].

Analogamente, accettare che milioni di persone su *Instagram* possano vedere e scaricare i contenuti pubblicati *open access*, non autorizza l'autorità investigativa a svolgere attività di controllo indiscriminato e continuativo[269]. D'altra parte, se può condividersi l'idea che le persone sacrifichino parte della propria intimità quando si trovano in luoghi pubblici, «ciò non significa che esse siano disposte a diventare "uomini di vetro"»[270]. Se così fosse, *Facebook*, al pari di ogni altro *social network*, rischierebbe di trasformarsi in un «*giant surveillance tool*» per il cui utilizzo «*no warrant [is] required*»[271].

Occorre considerare, peraltro, che i contenuti *open access* presenti nelle *social web-pages* riferibili a una determinata persona potrebbero essere stati pubblicati da soggetti diversi dall'interessato, come nel caso di un *tag* o di un *repost*, ovvero permanere nel cyberspazio anche contro la volontà del soggetto che li ha inizialmente immessi nella Rete[272]. Di conseguenza, e contrariamente a quanto si potrebbe pensare, la scelta di rendere liberamente disponibili certe informazioni, in un elevato numero di casi, non dipendere dalla volontà del

---

[266] È questa la tesi sostenuta da una parte della dottrina statunitense: cfr., per tutti, D.J. GLANCY, *Privacy on the Open Road*, in *Ohio Northern University Law Review*, 2004, p. 295 ss.; C. SLOBOGIN, *Public Privacy: Camera Surveillance fo public Places and the Right to Anonimity*, in *Mississipi Law Journal*, 2002, p. 13 ss.

[267] Per questa opinione, v. quanto efficacemente osservato da S. SIGNORATO, *Le indagini digitali*, cit., p. 83, secondo la quale «se un soggetto rivela volontariamente a persone che non conosce delle informazioni in un luogo digitale aperto al pubblico, non si potrà poi dolere che le medesime vengano visionate ed acquisite dalla polizia a fini investigativi, senza la necessità di alcun decreto autorizzativo da parte del pubblico ministero».

[268] È quanto sostenuto, del resto, con riguardo proprio alle attività di *data mining online*, da S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 323, per il quale «la crescita esponenziale delle informazioni disponibili […] determina un cambiamento di scala non soltanto quantitativo, ma qualitativo».

[269] Esplicitamente, in tal senso, v. A. LÒPEZ CABELLO – T.I. GRIFFA, *Privacidad en redes sociales y vigilancia* estatal, cit., p. 809; B.J. KOOPS, *Police Investigations in Internet Open Source*, cit., p. 655, per il quale «*Internet users may note generally expect the police scrutinise everything that roams on the Internet, particularly not if the investigations rely on sophisticated tools for mining open source*».

[270] G. DI PAOLO, *"Tecnologie del controllo" e prova* penale, cit., p. 174. Mostra di condividere tale lettura anche C. FANUELE, *La localizzazione* satellitare, cit., p. 39 che, a tal proposito, parla di «persone trasparenti».

[271] J. SEMITSU, *From Facebook to Mug Shot*, cit., p. 291. Per questa ragione, B.R. JOHNSON, *Untagging Ourselves: Facebook and the Law in the Virtual Panopticon*, in *Thomas M. Cooley Journal of Practical and Clinical Law*, 2011, p. 185 ss., si riferisce a *Facebook* come ad un vero e proprio «*virtual panopticon*».

[272] Trai rischi connessi all'utilizzo dei *social network* messi in luce dalla European Network and Information Security Agency (ENISA) nel già richiamato *report* titolato *Security issues and Recommendations for on line social networks*, 2007, cit., p. 8, vi è proprio la perdita di controllo sui dati immessi nelle piattaforme, anche laddove l'utente decida in seguito di modificare o eliminare il proprio *account*. In questi casi, infatti, le cd. informazioni secondarie, come, ad esempio, i commenti pubblici a *post* pubblicati da terzi rimarranno perlopiù *online*. A quanto detto, peraltro, si aggiunga che le *policy* predisposte dai gestori delle piattaforme risultano generalmente ambigue: *Facebook*, ad esempio, prevede che «Le informazioni rimosse possono persistere in copie di backup per un periodo di tempo ragionevole».

soggetto titolare delle stesse. In questa prospettiva, allora, si rivela quantomeno fuorviante l'insinuazione generalmente formulata dai detrattori della *privacy*: «se non volevi che i tuoi dati fossero conosciuti da terzi, perché li hai resi pubblici?»[273]. A tal proposito, si rivela parimenti infondata l'argomentazione secondo cui la mancata attivazione delle impostazioni di *privacy* a opera dell'utente – in grado di limitare la visibilità del suo profilo – rappresenterebbe un chiaro indice della volontà di rendere pubbliche le sue attività *online*. A sconfessare questo *modus pensandi* è stato, tra gli altri, l'*European Data Protection Board*. Nelle già richiamate Linee guida in tema di riconoscimento facciale, il Comitato ha espressamente affermato che le scelte compiute da un utente del *web*, specialmente se le *privacy settings* risultano affatto chiare e intellegibili, «*is not sufficient to consider that this data subject has manifestly made public its personal data*»[274].

La linea esegetica che si va esponendo trova un autorevole avallo nella giurisprudenza sovranazionale. Sin dal noto arresto *Rotaru* c. *Romania*[275], la Corte europea dei diritti dell'uomo, muovendo dall'esistenza di una «*zone of interaction of a person with others even in a public context*»[276], ha sottolineato che le informazioni pubbliche debbono essere considerate oggetto della tutela del diritto alla riservatezza quando sono sistematicamente raccolte e conservate in *database* detenuti dall'autorità giudiziaria[277]. In tale circostanza, l'attività di polizia provoca un'indebita interferenza con l'art. 8 CEDU, a prescindere dalla natura "pubblica" (*rectius*, *open access*) del dato e dal consenso liberamente prestato dal legittimo titolare. Consenso che, in nessun caso, può implicare una rinuncia ai diritti convenzionali tutelati dalla Carta. Viceversa, nel caso in cui la vigilanza non assuma i caratteri della sistematicità e non sia diretta a immagazzinare informazioni, nessuna violazione della *privacy* potrebbe essere ravvisata.

È interessante notare, peraltro, come la giurisprudenza della Corte di Strasburgo, sotto tale profilo, si collochi in perfetta linea di continuità con i *dicta* – invero, non sempre univoci e lineari – espressi dalla Corte Suprema americana. Sin dal risalente caso *Nader c. Gen. Motors Corp.*[278], i giudici d'oltreoceano hanno sottolineato che, mentre la «*mere observation*» condotta dalle autorità statali dei comportamenti tenuti dagli individui nei

[273] L. EDWARDS – L. URQUHART, *Privacy in Public Spaces*, cit., p. 15 (trad. nostra).

[274] EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, cit., par. 76.

[275] Corte edu, 4 maggio 2000, *Rotaru c. Romania*, par. 42-44.

[276] Corte edu, 24 giugno 2004, *Von Hannover c. Germania*, par. 50. Conforme, Corte edu, 28 aprile 2018, *Benedik c. Slovenia*, par. 100.

[277] Oltre ai due *leading cases* richiamati nelle precedenti note, v. Corte edu, 28 marzo 2003, *Peck c. Regno Unito*, par. 24; Corte edu, 6 giugno 2006, *Segerstedt-Wibers e altri c. Svezia*; Corte edu, 2 settembre 2010, *Uzun c. Germania*; Corte edu, 28 novembre 2017, *Antovic c. Montenegro*; Corte edu, 8 febbraio 2018, *Ben Faiza c. Francia*. Come sottolineano A. GAITO – S. FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, in A. Gaito (a cura di), *I principi europei del processo penale*, Roma, 2016, p. 370, la tutela apprestata dalla Corte al diritto alla riservatezza «si estende fino a comprendere l'acquisizione, con qualsiasi mezzo, di ogni elemento relativo allo svolgersi normale delle relazioni umane». Anche S. ALLEGREZZA, *Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione europea*, in D. Negri (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 69, mette in luce come «quello che rileva, però, non è tanto la pubblicità coeva dal dato personale, quanto la registrazione sistematica o permanente di quel comportamento».

[278] *Nader c. Gen. Motors Corp.*, 25 N.Y. 2d 560,570 (1970).

luoghi pubblici non costituisce un'invasione nella sfera della *privacy*, la sorveglianza continuativa, specialmente se eseguita per il tramite di strumentazioni elettroniche che consentono di conservare una grande quantità di informazioni, viola la ragionevole aspettativa di riservatezza dei cittadini[279]. È evidente, per quanto qui interessa, come l'analisi combinata e sistematica dei dati ricavati dai profili *open access* dei *social network* consenta all'autorità inquirente di creare un vero e proprio «*revealing montage of the user's life*»[280].

Per di più, la distinzione tra forme di *short search* e attività di *long-term surveillance* è stata messa in luce anche nelle *concurring opinions* rese dai giudici Alito e Sotomayor nel già menzionato caso *Stati Uniti c. Jones*. Facendo eco ad alcune considerazioni già espresse dalla Corte nella sentenza *Stati Uniti c. Knotts*[281], i due autorevoli magistrati hanno operato una distinzione tra un monitoraggio a breve termine dei movimenti di una persona su strade pubbliche, che non può ritenersi lesivo del IV emendamento e un monitoraggio (nel caso di specie, tramite GPS) a "lungo termine" che, per contro, incide in maniera significativa sulla privatezza dei dati personali[282]. In quest'ultimo caso, infatti, la *prolonged surveillance* è in grado di svelare tipologie di informazioni che «*can reveal more about a person than does any individual trip viewed in isolation*»[283].

In questa prospettiva, pertanto, la *repetitive examination* (o *repeated viewing*) dei profili *social* dell'indagato (o di un terzo), a differenza di visualizzazioni a carattere non sistematico, rappresenta una forma di *direct surveillance* altamente invasiva. Un'operazione, quest'ultima, che consente alla polizia giudiziaria di svolgere attività di *digital criminal profiling* attraverso la raccolta e l'elaborazione di una vastissima mole di informazioni relative alle abitudini di vita del soggetto, alle sue frequentazioni e ai suoi rapporti personali[284].

Le considerazioni svolte fino ad ora trovano un ulteriore e autorevole sostegno nel recente *report* dell'Alto Commissario per i Diritti Umani presso le Nazioni Unite, titolato «*The right to privacy in the digital age*»[285]. Nella parte dedicata all'impego di strumentazioni in grado di raccogliere, analizzare e archiviare grandi quantità di dati *online* presenti negli spazi pubblici virtuali e, in particolar modo, nei «*social media posts and the private and professional networks built on publicly accessible*», si afferma esplicitamente che la vigilanza sistematica delle attività realizzate in tali ambienti costituisce un'interferenza con il diritto alla *privacy* e può avere effetti pregiudizievoli nel godimento di altre libertà

[279] *Stati Uniti c. Powell*, 943 F. Supp. 2d 759, 776 (2013).

[280] *Stati Uniti c. Chavez*, 423 F. Suppl. 3d 194, 204-05 (W.D.N.C. 2019).

[281] *Stati Uniti c. Knotts*, 460 U.S. 276 (1983). La pronuncia appare significativa dal momento che, pur riconoscendo che «*a person traveling in an automobile on public thoroughfares has no resonable expectation of privacy in his movements from one place to another*», ha sottolineato la necessità di differenziare l'ipotesi *de qua* dal caso in cui l'autorità pubblica realizzi una forma di *long-term surveillance*. Sul punto, v. M. BEDI, *The Curious Case of Cell Phone Location Data: Fouth Amendament Doctrine Mash-Up*, in *Northwestern University Law Review*, 2015, p. 61 ss.

[282] La conclusione è stata nuovamente avallata, *ex multis*, in *Stati Uniti c. Graham*, 824 F. 3d 421, 435 (2016).

[283] *Stati Uniti c. Jones*, cit.

[284] Nella medesima prospettiva, v. M. O'FLOINN – D. ORMEROD, *Social Networking Sites, RIPA and Criminal Investigations*, in *The Criminal Law Review*, 2011, p. 774-779; F. SAMPSON, *Following the Breadcrums*, cit., p. 295 ss.

[285] REPORT OF THE OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS, *The right to privacy in the digital age*, 4 agosto 2022, spec., par. 43.

fondamentali. In assenza di una regolamentazione *ad hoc*, infatti, questa operazione sembra destinata ad arrecare un *vulnus* a quei "nuovi diritti"[286] elaborati nell'era tecnologica, tra i quali mette conto ricordare, specialmente, la libertà di movimento e di associazione in ambiente virtuale (intrinsecamente legate al diritto al pieno e libero sviluppo della personalità umana) e il diritto fondamentale a non essere permanentemente sorvegliato[287] che, in una moderna società democratica, costituisce la "versione 2.0" dei più tradizionali diritti alla intimità e alla protezione della vita privata[288].

A tal proposito, si rivelano, ancora una volta, illuminanti gli studi condotti nel contesto nordamericano dove, già da tempo, si è compreso come il semplice timore di essere sottoposti a un'attività di sorveglianza continuativa sui *social network* – così come in ogni altro spazio pubblico[289] – sia in grado di inibire il libero e pieno esercizio delle libertà fondamentali[290] (prima fra tutte, la libertà di autodeterminazione[291]), nonché di provocare una rinuncia ad avvalersi degli strumenti tecnologici per il timore di essere sottoposto a controllo continuativo[292]. In altre parole, la mera possibilità, ancorché teorica, che l'autorità investigativa possa liberamente osservare in maniera sistematica il comportamento *online* dell'utente, limita la sua libertà di scelta, di parola e di "movimento in ambiente virtuale", inducendone surrettiziamente un cambiamento dello stile di vita (cd. *panopticon effect* o *chilling effect*[293]). L'ordinamento, in tal modo, finisce per realizzare condotte di *stalking* occulto e dissimulato.

Alla luce di quanto osservato, è interessante dare conto del fatto che la distinzione tra sorveglianza occasionale – *rectius*, attività di apprensione di dati e informazioni – e vigilanza

---

[286] Cfr. Parte II, Cap. I.

[287] Prospettato, seppur implicitamente, da A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, cit., p. 633.

[288] «*The survival of democracy requires vibrant public spaces, both offline and online, where individuals can collaborate, organize, and go about their personal lives without fear of constant surveillance*» (FREEEDOM HOUSE, *Freeedom on the Net*, 2019, al sito *https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf.*).

[289] G. DI PAOLO, *"Tecnologie del controllo" e prova* penale, cit., p. 268, la quale sottolinea come «anche in assenza di atti che direttamente impediscono l'esercizio dei diritti fondamentali, l'idea di un pervasivo controllo da parte dell'autorità, effettivo o potenziale che sia, esercita sul piano psicologico una sottile forma di coercizione, che opera come potente effetto dissuasivo dall'esercizio delle libertà individuali». Anche a F. CAPRIOLI, *Riprese visive nel domicilio e intercettazione per immagini*, in *Giur. cost*., 2002, p. 2188, ritiene che le «pratiche investigative idonee a condizionare le scelte comportamentali di chi ne sia oggetto» incidono sulla libertà morale della persona. Nello stesso senso si esprime, ancorché con riguardo alle tecniche di riconoscimento facciale, J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen*., p. 1057 ss. e, spec., p. 1070.

[290] Quali, ad esempio, la libertà di manifestazione del pensiero, la libertà di culto e le libertà politiche.

[291] Si rivelano particolarmente interessanti, in proposito, le considerazioni di E. STOYCHEFF, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, in *Journalism & Mass Communication Quarterly*, 2016, p. 296 ss. In dottrina, peraltro, si è osservato che il ricorso a forme di sorveglianza aggregata, ancorché in forma anonima, «possieda comunque un impatto almeno indiretto sui diritti dell'individuo» (così, F. NICOLICCHIA, *Sorveglianza di massa e prerogative di riservatezza dell'individuo durante l'emergenza* SARS-CoV-2. *Scenari attuali e prospettive future*, in AA.VV., *Diritto virale: scenari e interpretazioni delle norme per l'emergenza* #Covid19, vol. I, Ferrara, 2020, p. 20).

[292] C. CONTI, *Sicurezza e riservatezza*, cit., p. 1575.

[293] Sulla capacità della sorveglianza *online* di incidere indirettamente sui comportamenti individuali, v. A. MARTHEWS – C.E. TUCKER, *The Impact of Online Surveillance on Behavior*, in D. Gray – S.E. Henderson (a cura di), *Cambridge Handbook of Surveillance Law*, Cambridge, 2017, p. 437 ss.; J.W. PENNEY, *Chilling Effects: Online Surveillance and Wikipedia*, in *Berkeley Tech Law Journal*, 2016, p. 117 ss.

continuativa condotta in relazione a informazioni *open access* reperibili nei *social network*, sia stata fatta propria da taluni ordinamenti stranieri, anche di diversa tradizione giuridica.

Nell'*Anteproyecto de ley orgánica de enjuiciamiento criminal* del 2020, ad esempio, il legislatore spagnolo, nel disciplinare espressamente l'attività della polizia giudiziaria diretta all'apprensione di informazioni disponibili in «*fuentes abiertas*», ha stabilito che la *policía judicial* può acquisire di propria iniziativa e senza previa autorizzazione «*todas aquellas informaciones relevantes para la investigación que se encuentren disponibles en fuentes abiertas de información*»[294]. Al contrario, nel caso in cui la raccolta di dati venga effettuata «*de forma sistemática y continuada con el objeto de crear un registro histórico de la actividad del investigado en el entorno digital*»[295], l'art. 516 del progetto di legge impone la preventiva autorizzazione del giudice istruttore. Come si legge nella relazione illustrativa[296], poiché il grado di intromissione nell'autodeterminazione informativa raggiunge, in quest'ultima ipotesi, un livello superiore rispetto all'acquisizione di dati *una tantum*, detta attività impone una tutela rafforzata (si legga, l'intervento giurisdizionale).

Appare parimenti emblematico, al riguardo, il radicale cambio di prospettiva che ha l'ordinamento d'oltremanica. Fino agli inizi del 2015 la letteratura era solita affermare che le informazioni pubblicamente disponibili nei *social network* non fossero coperte da una ragionevole aspettativa di *privacy*. Di conseguenza, si ammetteva la possibilità che la polizia giudiziaria potesse utilizzare la tecnologia SOCMINT per accedere e conservare i dati, pur in assenza di una *prior authorisation*[297]. Recentemente, però, la nuova consapevolezza circa l'importanza che la *privacy* ha via via assunto anche nei "luoghi pubblici virtuali" sembra aver fatto breccia, se non tra gli studiosi della materia, quantomeno a livello istituzionale. In proposito, numerosi *Districts Council* hanno adottato protocolli e linee guida per l'utilizzo dei *social network* nel corso delle indagini penali[298], stabilendo, a chiare lettere, che la visione ripetuta e regolare di informazioni *open source*, a differenza di una visualizzazione sporadica, costituisce una forma di sorveglianza diretta e, perciò, impone agli organi d'indagine di ottenere un'autorizzazione preventiva ai sensi del *Regulation of Investigatory Powers Act* (RIPA)[299].

---

[294] Art. 514, comma 1, *Anteproyecto de ley orgánica de enjuiciamiento criminal*, 2020.

[295] Art. 514, comma 2, *Anteproyecto de ley orgánica de enjuiciamiento criminal*, 2020, cit.

[296] Memoria del Análisis de Impacto Normativo, *Anteproyecto de ley orgánica de enjuiciamiento criminal*, 2020, gennaio 2021, al sito *https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/210126%20MAIN%20LECRIM%202020%20INFORMACION%20PUBLICA.pdf*.

[297] M. O'FLOINN – D. ORMEROD, *Social Networking Sites, RIPA and Criminal Investigations*, cit., p. 766 ss.

[298] Cfr., ad es., Arun District Council, *Guidance on the Use of Social Media in Investigations*, ottobre 2019; Colchester Use of Social Media in Investigations District Council, *Use of Social Media in Investigations Policy and Procedure 2021/22*, novembre 2021; Stratford-on-Avon District Council, *Use of Social Media in Investigations Procedure*, dicembre 2020; Coventry District Council, *Use of Social Media in Investigations Guidance*, agosto 2018.

[299] L'art. 48, comma 2, del *Regulation of Investigatory Powers Act* (RIPA), include espressamente nel concetto di sorveglianza le seguenti attività: «*a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications; b) recording anything monitored, observed or listened to in the course of surveillance; c) surveillance by or with the assistance of a surveillance device*».

7.1 La veste giuridica del *cyberpatrolling* investigativo e l'(in)utilizzabilità delle informazioni raccolte

Fin qui si è sostenuto che, mentre il *cyberpatrolling* occasionale non attribuisce alcuna ragionevole aspettativa di *privacy* nei confronti dell'autorità statale, la raccolta continuativa e occulta di contenuti *open source* pubblicati nei *social network*, per contro, è un'operazione potenzialmente in grado di incide in modo significativo sulle libertà fondamentali dell'indagato (e dei terzi eventualmente interessati o coinvolti).

Ribadito che l'attività qui in esame risulta del tutto sfornita di una disciplina legale, si pone, a questo punto, il tema della individuazione della sua qualificazione giuridica, onde verificare l'eventuale riconducibilità, in via interpretativa, a un atto di indagine tipico e nominato.

La risposta a quest'ultimo quesito parrebbe negativa, per diverse e concorrenti ragioni che si tenterà subito di illustrare.

Non sembra possibile, in primo luogo, collocare l'attività di monitoraggio di cui si discute nell'alveo della disciplina delle intercettazioni di comunicazioni informatiche o telematiche contenuta agli artt. 266-*bis* ss. c.p.p., neppure quando il contenuto appreso abbia natura comunicativa e goda, perciò, della tutela prevista dall'art. 15 Cost. Vi osta, senza ombra di dubbio, la "vocazione pubblica" del dato e la mancanza della volontà di escludere terzi dalla conversazione; requisiti, come noto, indispensabili per ricondurre la captazione nell'alveo delle intercettazioni[300].

Né, del resto, il *cyberpatrolling* può essere assimilato a un'ispezione personale, poiché, a differenza di quest'ultima, esso non mira, necessariamente, ad accertare le tracce e gli altri effetti materiali del reato, né, tantomeno, a descrivere lo stato attuale dei luoghi. Per di più, mentre il *social media monitoring* implica una compressione della riservatezza, l'atto investigativo disciplinato agli artt. 244 ss. c.p.p. incide direttamente sulla libertà personale tutelata all'art. 13 Cost.

Parimenti eccentrico sembrerebbe, altresì, il tentativo di ricondurre l'atto in esame nella categoria delle perquisizioni, tanto tradizionali, quanto informatiche.

In primo luogo, gli artt. 247 ss. c.p.p. disciplinano un mezzo investigativo strutturalmente concepito per la ricerca del corpo del reato o delle cose pertinenti al reato nel mondo fisico. Al contrario, la *social network surveillance* prescinde da una ricerca così indirizzata e si svolge esclusivamente in ambiente virtuale. In secondo luogo, mentre le perquisizioni "ordinarie", atto investigativo "istantaneo", consentono alla polizia giudiziaria di acquisire solamente materiale probatorio esistente *in rerum natura* anteriormente al compimento dell'atto, il carattere continuativo e la vocazione "ultrattiva" del *cyberpatrolling*, per contro, consentono l'apprensione anche di dati venutisi a creare successivamente rispetto all'inizio delle operazioni di vigilanza. Evidente è, perciò, il differente grado di intrusività degli

[300] …in ossequio alla definizione offerta da Cass. pen., Sez. Un., 24 settembre 2003, n. 36747. Per le medesime conclusioni, v., con riguardo ai messaggi scambiati pubblicamente in *Internet*, S. SIGNORATO, *Le indagini digitali*, cit., p. 251; G. VACIAGO, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012, p. 119; e, per quanto concerne le informazioni pubblicate volontariamente nei *social network*, T. ARMENTA DEU, *Regulación legal y valoración probatoria de fuentes de prueba digital*, cit., p. 74.

strumenti in esame. Senza voler considerare, infine, che l'attività di perquisizione tradizionale, pur essendo un atto a sorpresa, è destinato a divenire "palese" (si legga, conosciuto all'indagato) nel momento della sua concreta realizzazione, tanto che la legge prevede una serie di adempimenti in funzione di garanzia (art. 365 c.p.p.)[301]. Il *cyberpatrolling*, per converso, è sì un atto a sorpresa, ma, soprattutto, un'operazione eseguita in maniera occulta e segreta per tutto il corso del suo svolgimento.

Esclusa, dunque, ogni ipotetica assimilazione della SOCMINT a operazioni di indagine tipizzate, non resta che vagliarne la riconducibilità nell'ambito delle attività di ricerca della prova atipiche.

Introdotto con l'obiettivo di assicurare un processo penale "al passo con i tempi", l'art. 189 c.p.p. ha rappresentato, com'è noto, «una scelta intermedia»[302] tra principi collocati ai due estremi ideali: tassatività e libertà dei mezzi di prova[303]. Vera e propria "norma di chiusura", la disposizione è stata pensata dal codificatore per consente di adeguare il sistema probatorio all'evoluzione e allo sviluppo di nuove tecniche scientifiche e tecnologiche. Il codice del 1988 ha, però, subordinato l'ammissione di prove non disciplinate dalla legge (*rectius*, prove innominate che il legislatore non ha espressamente contemplato «perché imprevedibili»[304]), alla presenza di specifici requisiti: l'idoneità ad assicurare l'accertamento dei fatti, la tutela della libertà morale del soggetto e la necessità di un contraddittorio preventivo tra le parti circa la modalità di assunzione della prova.

Orbene, nel silenzio della norma, la dottrina si è fin da subito interrogata circa la possibilità di estendere l'ambito di applicazione dell'art. 189 c.p.p. anche ai mezzi di ricerca della prova non tipizzati, con l'obiettivo di introdurre, in via interpretativa, un principio di atipicità delle indagini preliminari.

La questione, come noto, è tutt'ora dibattuta.

Stando a una prima corrente di pensiero[305], l'esclusione si giustificherebbe, anzitutto, alla luce di un'interpretazione letterale: l'utilizzo del termine "assunzione" evoca i concetti di "contraddittorio", "dibattimento" e, dunque, di "prova"; al contrario, quando il codice di rito tratta dei "mezzi di ricerca della prova", vengono impiegate espressioni e, quindi, concetti

---

[301] S. MARCOLINI, *Le cosiddette perquisizioni* online, cit., p. 2859.

[302] Relazione al progetto preliminare del codice di procedura penale, in Gazz. Uff., suppl. ord. n. 2, 24 ottobre 1988, Serie gen., p. 60.

[303] Per un'analisi, anche storica, sull'alternarsi di queste due concezioni, si rinvia a E. ZAPPALÀ, *Il principio di tassatività dei mezzi di prova nel processo penale*, Milano, 1982, *passim*.

[304] R. ORLANDI, *Atti e informazioni della autorità amministrativa nel processo penale. Contributo allo studio delle prove extracostituite*, Milano, 1992, p. 24. Come sottolineato da M. NOBILI, *La nuova procedura penale. Lezioni agli studenti*, Bologna, 1989, p. 120, occorre «essere fermissimi, almeno dal punto di vista dei principi, nel sottolineare che l'articolo 189 c.p.p., innegabilmente pericoloso da punto di vista pratico, non equivale affatto a giustificare maggiori e ulteriori libertà nella formazione della prove già regolamentate».

[305] Tra i sostenitori di questa linea esegetica, v. O. MAZZA, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont. – Riv. Trim.*, 2013, 3, p. 9; F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., p. 12 ss.; N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Padova, 1992, p. 213; L. FILIPPI, *L'*home watching: *documento, prova atipica o prova incostituzionale?*, in *Dir. pen. proc*., 2001, p. 95; S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2015, p. 774.

differenti, quali, ad esempio, quello di "elementi probatori"[306]. Inoltre, la previsione di un contraddittorio preventivo sulle modalità di assunzione renderebbe incompatibile l'art. 189 c.p.p. con tutti quei mezzi di ricerca della prova occulti e a sorpresa per i quali l'assenza di preavviso dell'atto e di conoscenza del contenuto da parte dell'interessato costituiscono *condicio sine qua non* della loro efficacia e delle genuinità del dato raccolto[307].

Tali argomentazioni, però, non hanno convinto la maggior parte della dottrina[308] che, al contrario, valorizzando argomenti di carattere sistematico, sottolinea come l'art. 189 c.p.p. sia collocato tra le disposizioni generali del Libro III dedicato alle prove – *lato sensu* intese –, nel quale vengono disciplinati tanto i mezzi di prova, quanto i mezzi di ricerca della prova. Con riguardo, poi, alla necessità di garantire, in ogni caso, un contraddittorio tra le parti, alcuni autori hanno sostenuto la possibilità di realizzare un confronto a posteriori avente a oggetto la sussistenza dei requisiti di ammissibilità imposti dalla legge[309]. A favore della tesi maggioritaria, peraltro, sembrerebbe deporre anche il richiamo testuale operato dalla Relazione al Progetto preliminare del codice di procedura penale, laddove si afferma che la disposizione in parola è stata pensata per far fronte al continuo sviluppo tecnologico che estende le «frontiere dell'investigazione»[310].

Al netto di tale dibattito dottrinale, deve riconoscersi che l'art. 189 c.p.p. ha ormai assunto le sembianze di una "norma contenitore" alla quale dottrina e giurisprudenza ricorrono nel disperato tentativo di legittimare tutte quelle nuove tipologie investigative non disciplinate dalla legge[311]. In tal modo, però, non solo si finisce per eludere i limiti imposti dal legislatore al momento di disciplinare modalità tipiche di ricerca della prova, ma si rischia – e il caso del *cyberpatrolling* ne è una plastica esemplificazione – di attribuire un potere arbitrario alla

---

[306] L'argomento testuale, però, appare debole: l'impiego del termine assunzione non è risolutivo, posto che il legislatore potrebbe non averlo inteso in senso strettamente tecnico, come accade, ad esempio, anche nella rubrica dell'articolo 188 c.p.p. «libertà morale nell'assunzione della prova», norma che la dottrina riferisce unanimemente anche agli atti investigativi (in questo senso, v., condividendone l'opinione, S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, p. 580 ss.).

[307] A conforto dell'esegesi in parola, si è recentemente sostenuto che la tipologia di bilanciamento cui ricorre il legislatore nel regolamentare le contrapposte esigenze in tema di mezzi di prova non sarebbe estendibile anche agli atti di indagine. Più nello specifico, l'art. 189 subordina l'amissione delle prove innominate alla verifica circa la loro validità gnoseologica e all'espletamento di un contraddittorio tra le parti. Al contrario, il giudizio che dovrebbe essere astrattamente condotto con riguardo agli atti di indagine atipici riguarda la necessità di trovare un punto di equilibrio tra l'efficacia dell'atto e i diritti fondamentali dei soggetti coinvolti. In quest'ultimo caso, dunque, appare irrilevante la capacità probante dell'atto, elemento qualificante il giudizio di bilanciamento relativo ai mezzi di prova (F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., p. 12 s.).

[308] La tesi è avallata, tra i molti, da F.R. DINACCI, *L'inutilizzabilità nel processo penale. Struttura e funzioni del vizio*, Milano, 2008, p. 60, nt. 69; M. NOBILI, sub *Art. 189 c.p.p.*, in M. Chiavario (a cura di), *Commento al nuovo codice di procedura penale*, Vol. II, Torino, 1990, p. 399 ss.; C. CONTI, *Accertamento del fatto e inutilizzabilità*, cit., p. 160. In questo senso è orientata anche la giurisprudenza: cfr. Cass., Sez. Un., 28 marzo 2006, n. 26795, cit.

[309] Tra i primi a proporre questa lettura, A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle "prove incostituzionali"*, in *Cass. pen.*, 1999, p. 1195. In realtà, lo stesso A. ha recentemente riconosciuto come ancorché si possa spostare il contraddittorio più avanti – in dibattimento, quando la prova viene ammessa – ciò non equivale a garantire un contraddittorio *ex ante* (ID., *La fase che "non conta e non pesa"*, cit., p. 113).

[310] Relazione al progetto preliminare del codice di procedura penale, cit., p. 60.

[311] Come sottolinea D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità* p. 26, quando «la prassi poliziesca scopre e collauda tecniche investigative inedite, la giurisprudenza tende a qualificarle superficialmente alla stregua di mezzi atipici ma al contempo legittimi di ricerca probatoria».

polizia giudiziaria nel compimento di attività investigative. Al contrario, nel corso delle indagini preliminari, è bene ribadirlo con forza, il principio di massima espansione dei diritti di libertà[312] e il canone di legalità processuale impongono di affermare che qualunque operazione investigativa non espressamente consentita dalla legge che incide sui diritti fondamentali della persona deve ritenersi vietata[313].

In questa prospettiva, e volendo accogliere l'approccio maggioritario poc'anzi richiamato, occorre stabilire se l'attività di *cyberpatrolling* investigativo risulti conforme o meno alle condizioni di ammissibilità dettate dall'art. 189 c.p.p.

Quanto al primo requisito, può forse dubitarsi dell'astratta idoneità di questo mezzo di ricerca della prova di «consentire un'obiettiva ricostruzione della vicenda storica»[314], poiché, come si è detto, le informazioni *open access* non sono, per loro stessa natura, necessariamente affidabili e accurate[315].

Anche il secondo parametro previsto all'art. 189 c.p.p. sembra prospettare profili problematici di non poco momento. Se correttamente inteso, infatti, esso impone di escludere dal compendio degli strumenti utilizzabili tutte quelle «pratiche investigative idonee a condizionare le scelte comportamentali di chi ne sia oggetto»[316]; un condizionamento che, alla luce della natura preventivo-cautelativa della disposizione, rileva anche in termini meramente potenziali[317]. A tale riguardo, si è già avuto modo di ricordare come il semplice timore di essere assoggettati a operazioni di sorveglianza continuativa via *web* possa indurre gli individui a mutare le proprie abitudini di vita, influendo così sul concreto esercizio della libertà di autodeterminazione[318]. In proposito, peraltro, a nulla varrebbe obiettare che l'accoglimento di una simile interpretazione finirebbe per considerare illegittimi tutti i mezzi

---

[312] Cfr. Parte II, Cap. I.

[313] Richiamando l'efficace formula utilizzata da F. RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001, p. 65, si può affermare che «all'autorità giudiziaria, è vietato qualsiasi atto che incida sui diritti della persona, tranne ciò che è esplicitamente permesso». Secondo l'A., infatti, «all'interprete è precluso estendere, oltre i casi consentiti, le ipotesi in cui solo eccezionalmente la pubblica autorità ha il potere di limitare i diritti di libertà al fine di soddisfare le esigenze della persecuzione penale» (p. 67).

[314] Questo è il significato attribuito al criterio di idoneità dalla dottrina maggioritaria. Si veda, per tutti, G.F. RICCI, *Le prove atipiche*, Milano, 1999, p. 535.

[315] In termini non dissimili, v. E. DE BUSSER, *Open Source Data and Criminal Investigations*, cit., p. 98.

[316] F. CAPRIOLI, *Riprese visive nel domicilio*, cit., p. 2191.

[317] G.F. RICCI, *Le prove atipiche*, cit., p. 535.

[318] Il tema, non è fuor d'opera ricordarlo, è oggetto di ampio dibattito anche nel contesto del pedinamento satellitare. In quella sede, la dottrina maggioritaria ritiene che non sussista alcuna menomazione della libertà di autodeterminazione poiché il bersaglio è del tutto ignaro di essere seguito (per questa opinione, v., *ex plurimis*, T. BENE, *Il pedinamento elettronico*, cit., p. 453, nt. 37; C. CONTI, *Accertamento del fatto e inutilizzabilità*, cit., p. 239; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007, p. 241; S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, cit., p. 593. Nello stesso senso è orientata la giurisprudenza di legittimità: cfr., ad es., Cass. pen., Sez. II, 30 ottobre 2008, in *Guida dir.*, 2009, 5, p. 90). Al contrario, altri autori sottolineano come il timore di essere sottoposti a controllo occulto e continuativo provochi un *vulnus* alla libertà di autodeterminazione (C. FANUELE, *La localizzazione* satellitare, cit., p. 30 s.; F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., p. 79).

Medesimi dubbi interpretativi, invero, sono emersi anche con riguardo all'astratta riconducibilità delle videoriprese nell'ambito della fattispecie contemplata all'art. 189 c.p.p. Nel senso che non «può ritenersi condizionato nel proprio agire chi ignori di essere sottoposto ad un controllo occulto», C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 209; F. CAPRIOLI, *Riprese visive nel domicilio*, cit., p. 2188. *Contra*, L. FILIPPI, *L'*home watching, cit., p. 96.

tipici di ricerca della prova caratterizzati da una componente *lato sensu* occulta, come nel caso delle intercettazioni. In questa ultima ipotesi, il cittadino, stante la vigenza di una previsione normativa espressa che individua casi e modi della limitazione del diritto fondamentale, è pienamente consapevole che l'autorità giudiziaria, nei casi e con i limiti previsti, appunto, dalla legge ha la possibilità di captare le conversazioni dallo stesso intrattenute.

A questo punto dell'analisi, però, un ulteriore quesito sorge spontaneo: anche qualora si ritenessero integrati i requisiti previsti all'art. 189 c.p.p., occorrerebbe chiedersi se il *cyberpatrolling* investigativo comprima o meno uno dei diritti fondamentali sanciti nella Carta delle Leggi; e, in caso di risposta affermativa, se e quali conseguenze possano derivarne sul versante dell'utilizzabilità probatoria del materiale raccolto.

A tale riguardo, si è visto come l'impiego del *social network monitoring* provochi una compressione della *privacy*; un diritto, quest'ultimo, che, a seguito degli impulsi provenienti dalla giurisprudenza europea, è destinato a trovare pieno riconoscimento anche nei "luoghi pubblici" ogniqualvolta l'autorità statale realizzi attività di controllo continuativo e occulto. In questo senso, non sembra peregrino ipotizzare l'affermarsi, nella realtà dei *social network*, di una nuova componente della privatezza che potrebbe essere denominata "diritto a non veder tracciate continuativamente le proprie attività pubbliche *online*"[319]. Una sorta di "*right do no track*" di matrice convenzionale che, acquisendo valore anche in una prospettiva nazionale, è volto a limitare tutte quelle attività investigative che si estrinsecano in una raccolta massiva e sistematica di informazioni *open access*.

Accertata, dunque, la violazione di una libertà fondamentale, l'attenzione parrebbe doversi rivolgere al tema delle prove incostituzionali, cioè quei mezzi di prova (e, per estensione, mezzi di ricerca della prova) non disciplinati dalla legge che consentono di acquisire elementi informativi con modalità lesive dei diritti dell'individuo tutelati nella Carta Suprema[320].

In realtà, però, non sembra necessario scomodare una categoria concettuale tanto complessa e tutt'ora foriera di incertezze dogmatiche. Del resto, anche laddove si ritenga di conferire diritto di cittadinanza alla cd. inutilizzabilità costituzionale, essa sarebbe chiamata a operare solo in presenza di un *vulnus* ingiustificato a un diritto fondamentale garantito dalla Carta e, più in particolare, alle libertà previste dagli artt. 13 ss. Cost. Solo in questi casi, infatti, l'inosservanza della "doppia riserva" giustificherebbe l'inutilizzabilità del materiale acquisito. Sennonché, la *privacy*, lo si è visto, non trova espresso riconoscimento

[319] Lo spunto per l'enunciazione di questa nuova componente digitale della *privacy* è offerto dalla lettura di uno stimolante passaggio dell'opera di S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 398-404.

[320] La messa a punto della categoria concettuale, com'è noto, si deve a V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1973, p. 341 ss., a commento della fondamentale pronuncia Corte cost., 6 aprile 1973, n. 34, in *ivi*, 1973, p. 316 ss. Sul tema della prova incostituzionale, cfr., per una panoramica generale, F.R. DINACCI, *L'inutilizzabilità nel processo penale*, cit., p.75-82; C. CONTI, *Accertamento del fatto e inutilizzabilità*, cit., p. 150 ss.; F. CORDERO, *Tre studi sulle prove penali*, Milano, 1963, p. 145 ss.; F. CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, p. 236-247; N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, cit., p. 204 ss.; e, con specifico riguardo alla prova incostituzionale calata nelle peculiarità della *digital evidence*, S. MARCOLINI, *Regole di esclusione costituzionali e nuove tecnologie*, in *Criminalia*, 2006, p. 387 ss.; M. PITTIRUTI, Digital evidence *e procedimento penale*, cit., p. 148-155.

costituzionale, a meno di non volerla ricondurre (pur condivisibilmente) nella previsione dell'art. 2 Cost.[321], il quale, però, non prevede, in ogni caso, né una riserva di legge, né, tantomeno, una riserva di giurisdizione. *Rebus sic stantibus*, la violazione della riservatezza, sotto il profilo che qui interessa, sembra destinata all'irrilevanza processuale e alla soccombenza rispetto alla tutela del principio di efficacia investigativa[322].

È a questo punto dell'analisi, però, che sembrano assumere un certo vigore ermeneutico gli artt. 8 CEDU, 7 e 8 della Carta dei diritti fondamentali dell'UE (Carta di Nizza), disposizioni che costituiscono il parametro normativo utilizzato dalle Corti europee per saggiare la legittimità delle intrusioni nella vita privata delle attività realizzate dalle autorità statali (di polizia o giudiziarie). L'enunciato pattizio, in particolare, ha assunto, per effetto delle cd. "sentenze gemelle", il rango di norma interposta, cosicché deve ritenersi direttamente applicabile nell'ordinamento italiano per effetto dell'art. 117 Cost.[323].

Ebbene, la norma convenzionale, dopo aver proclamato il diritto al rispetto della vita privata e familiare, ne subordina l'ingerenza da parte di un'autorità pubblica alla previsione di una riserva di legge o, meglio, una proporzionalità in astratto (*i*), in base a un criterio di stretta necessità (*ii*)[324], per il perseguimento di uno tra gli scopi legittimi indicati al secondo paragrafo della stessa disposizione (*iii*).

È noto, sul primo versante (*i*), l'atteggiamento assunto dalla Corte di Strasburgo: la locuzione «*law*» dev'essere intesa nel senso sostanziale del termine, e cioè quale necessità di un'idonea base legale a livello nazionale, potendo questa essere ricavata tanto da una consolidata interpretazione giurisprudenziale (diritto vivente), quanto da un atto normativo di fonte primaria o a essa subordinato[325]. L'esegesi estensiva, com'è intuibile, si giustifica tenendo conto del fatto che i giudici europei sono chiamati a individuare un punto di equilibrio tra le differenti tradizioni giuridiche che contraddistinguono i Paesi della "grande Europa": *common law* e *civil law*. Ciò nondimeno, in un sistema, come quello italiano, di tipo continentale governato dal principio di legalità cd. «legicentrica»[326], la riserva di legge alla quale si riferisce l'art. 8 CEDU non può che essere intesa in termini *stricto sensu* formali, dovendosi categoricamente escludere la possibilità che un orientamento pretorio, per quanto consolidato o granitico, possa ritenersi sufficiente a giustificare una limitazione della

[321] Cfr. Parte II, Cap. I.

[322] Avalla questa conclusione, con riguardo alle prove innominate *ex* art. 189 c.p.p. lesive della riservatezza, ad es., L. BELVINI, *Principio di proporzionalità e attività investigativa*, cit., p. 165.

[323] Corte cost., 22 ottobre 2007, n. 348 e Corte cost., 22 ottobre 2007, n. 349, sulle quali v., per tutti, M. CARTABIA, *Le sentenze gemelle: diritti fondamentali, fonti, giudici*, in *Giur. cost.*, 2007, p. 3564 ss.

[324] Così dev'essere intesa l'espressione «costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute e della morale, o alla protezione dei diritti e delle libertà altrui». In proposito, cfr. Corte edu, 18 settembre 2014, *Brunet c. Francia*, par. 32 ss.; Corte edu, 29 luglio 2010, *Agraw c. Svizzera*, par. 44.

[325] Cfr. Corte edu, 25 marzo 1985, *Silver e altri c. Regno Unito*; Corte edu, 24 aprile 1990, *Kruslin c. Francia*, par. 28 ss.

[326] M. VOGLIOTTI, voce *Legalità*, in *Enc. dir.*, Annali IX, Milano, 2013, p. 373.

privacy[327] e, più in generale, di qualunque diritto fondamentale[328]. Ancorché autorevole dottrina abbia prospettato la necessità di ripensare, in una logica *fuzzy* o *flow*, il canone di stretta legalità alla luce del nuovo paradigma plurale, eterogeneo e dinamico di matrice europea[329], nell'attuale sistema penalprocessuale italiano «*il nullum crimen sine lege* non ha […] ceduto il posto al *nullum crimen sine iure*»[330]. Il giusto processo, come si ricava dal dettato letterale dell'art. 111, comma 1 Cost., è «regolato» solo ed esclusivamente «dalla legge», intesa come «entità estranea, "altra", se non addirittura contrapposta, rispetto a chi deve applicarla»[331].

In merito, poi, agli scopi legittimanti l'intrusione (*ii*), l'art. 8, par. 2, individua, tra i molti, la tutela della «sicurezza nazionale» e della «prevenzione del crimine». A tal proposito, non v'è dubbio che la necessità di garantire la *tranquillitas* collettiva mediante un'efficace attività di prevenzione e repressione penale costituisca un obiettivo più che legittimo[332], tanto che la Corte, nelle pronunce più recenti, ha tendenzialmente accettato che detto scopo possa giustificare «l'uso di nuove tecnologie nella sorveglianza segreta delle persone, senza troppo fermarsi a verificare se, effettivamente, l'obiettivo perseguito nella specie fosse tale»[333].

Malgrado ciò, va sottolineato come l'enunciazione degli scopi fissati dalla disposizione pattizia – trai quali è ricompreso, come detto, quello della repressione penale – non possa legittimare, di per sé, l'ingerenza nella *privacy* dei cittadini. L'inciso «*in a democratic*

---

[327] In questo senso, v. S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico*, cit., p. 2865; A. CAMON, voce *captazione di immagini* (dir. proc. pen.), in *Enc. dir.*, Annali VI, Milano, 2013, p. 145.

[328] Con plastica efficacia, F. CAPRIOLI, *Il giudice e la legge processuale: il paradigma rovesciato*, in *Ind. pen.*, 2017, p. 967, sottolinea come «sottratta al governo della legge e affidata al governo degli uomini, la tutela dei diritti fondamentali – oltre a perdere legittimazione politica – si fa estemporanea, arbitraria, effimera. Nessuna autentica certezza dei diritti interviene a rimpiazzare la claudicante certezza del diritto».

[329] È la tesi notoriamente avanzata da R.E. KOSTORIS, *Processo penale, diritto europeo e nuovi paradigmi del pluralismo giuridico postmoderno*, in *Riv. it. dir. proc. pen.*, 2015, p. 1177 ss. e, spec., p. 1193, ove l'A. sottolinea come il diritto europeo abbia portato a una profonda erosione del modello continentale «sia perché le "leggi" che vengono in gioco, anche in materia di giustizia penale, sono […] molteplici e di varia provenienza, e il codice è solo una di queste, sia perché i nuovi assetti segnano una transizione sempre più marcata da una legalità di tipo "statico", prevalentemente "normativa" a una legalità "europea" di tipo dinamico, prevalentemente "giurisprudenziale"». L'impostazione è avversata, con viva efficacia, da O. MAZZA, *Tradimenti di un codice*, cit., p. 107 ss. A favore di una concezione "forte" della legalità processuale si mostra anche D. NEGRI, *Splendori e miserie della legalità processuale. Genealogie culturali,* èthos *delle fonti, dialettica tra le Corti*, in *Arch. pen.*, 2017, p. 421 ss.

[330] Così, assai efficacemente, G. AMARELLI, *Dalla legolatria alla post-legalità: eclissi o rinnovamento di un principio?*, in *Riv. it. dir. proc. pen.*, 2018, p. 1444.

[331] M. NOBILI, *Principio di legalità e processo penale (ricordando Franco Bricola)*, in *Riv. it. dir. proc. pen.*, 1995, p. 650.

[332] E, in effetti, si è soliti ritenere la tutela della *privacy* recessiva rispetto all'esigenza di accertamento. Le indagini penali, in questo senso, nient'altro sarebbero se non una forma di "attentato legalizzato" ai valori della riservatezza. Per questa impostazione, v. S. CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in D. Negri (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, cit., p. 6, per la quale «l'obbligo di accertamento delle responsabilità, fa scivolare in secondo piano l'esigenza soggettiva di impedire intrusioni nella vita privata» e, dunque, questa finisce «per soccombere di fronte al soverchiante interesse alla repressione dei reati e alla punizione dei colpevoli»; F. CENTORAME, *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. it. dir. proc. pen*., 2021, p. 501. In questi termini, esplicitamente, Cass. pen., Sez. II, 21 aprile 2017, n. 28367; Cass. pen., Sez. II, 8 marzo 2018, n. 22169.

[333] L. SEMINARA, *Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani*, in *Rivista diritto dei media*, 2018, 2, p. 140.

society», infatti, costituisce il limite entro cui l'ordimento nazionale può legittimamente menomare il diritto alla riservatezza per il perseguimento di quegli obiettivi fissati *ex ante* dalla legge. Diversamente opinando, vi sarebbe il rischio di «minare o addirittura distruggere la democrazia che si presume di difendere»[334].

Anche qualora la misura di sorveglianza segreta si rivelasse idonea a perseguire uno scopo legittimo, i mezzi utilizzati dovrebbero essere comunque necessari e proporzionati (*iii*), nel senso che l'ingerenza nel bene giuridico tutelato (*rectius*, la riservatezza) dovrebbe risultare indispensabile e, al contempo, parametrata al perseguimento di quegli obiettivi indicati dalla legge (prevenzione e repressione criminale). È ben noto, del resto, come il canone *de quo* vada assumendo un ruolo tutt'altro che secondario nell'ambito delle indagini penali digitali lesive della *privacy*[335], specialmente a fronte di strumenti acquisitivi, come quello in esame, diretti all'apprensione di informazioni che, se valutate singolarmente, presentano un carattere evanescente, ma, se trattate in maniera massiccia e sistematica, acquistano una certa consistenza tanto in termini di "utilità investigativa", quanto di intrusività nei diritti fondamentali[336].

Alla luce di quanto osservato, dunque, pare potersi affermare che l'attività di *cyberpatrolling* realizzata nel contesto italiano per finalità di repressione dei reati contrasti con l'art. 8 CEDU, stante l'assenza di un quadro normativo chiaro e preciso che indichi casi e modi di limitazione del diritto *ivi* sancito.

Quanto detto, però, non è sufficiente a far calare il sipario sul tema *de quo*.

Anche volendo riconoscere l'immediata operatività della disposizione pattizia nell'ordinamento interno per effetto della "clausola di interposizione" prevista all'art. 117 Cost., occorre chiedersi se il dettato normativo sia in grado di giustificare un'inutilizzabilità di derivazione comunitaria (cd. prova inconvenzionale). A tal proposito, ben potrebbe spendersi l'argomentazione analogica. Facendo leva sulla nota esegesi richiamata a sostegno dell'inutilizzabilità delle prove assunte *contra Constitutionem*, sarebbe possibile offrire una lettura convenzionalmente orientata dell'art. 191 c.p.p., includendo nel concetto di «legge» non solo la fonte costituzionale[337], ma anche quella convenzionale[338].

La tesi, però, rischia di esporsi alle medesime critiche già spese da una parte della dottrina, tanto sul piano letterale quanto sostanziale, allorquando si è messo in luce come la Carta Fondamentale costituisca una semplice tavola di valori, inidonea a giustificare divieti probatori immediatamente operativi sul piano codicistico, in assenza di una intermediazione legislativa[339]; ciò che difetterebbe, in altri termini, è il nodo di congiunzione tra l'enunciato

---

[334] Corte edu, 24 ottobre 1983, *Silver e altri c. Regno Unito*, cit., par. 97 (trad. nostra).

[335] Cfr., per tutti, L. BELVINI, *Principio di proporzionalità e attività investigativa*, cit., p. 91 ss.; F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Dir. pen. cont*., 8 gennaio 2018, p. 1 ss.

[336] La considerazione è offerta da V. BONINI, *Videoriprese investigative*, cit., p. 346.

[337] Per tale opinione con riguardo alla prova incostituzionale, v. A. CAMON, *Le riprese visive come mezzo d'indagine*, cit., p. 1188; L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, p. 97 ss.

[338] La tesi è avallata, *ex multis*, da F. GIUNCHEDI, *Captazioni "anomale" di comunicazioni: prova incostituzionale o mera attività di indagine?*, in *Proc. pen. giust.*, 2014, 5, p. 137; S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico*, cit., p. 760 ss.; F. TRAPELLA, *Equo processo e inutilizzabilità tra codice e C.E.D.U.*, in *Arch. pen*., 2020, p. 778 s.; P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 339.

[339] C. CONTI, *Accertamento del fatto e inutilizzabilità*, cit., p. 154.

costituzionale (o convenzionale) e la regola di esclusione probatoria. Per di più, occorre ricordare come la giurisprudenza europea abbia assunto un orientamento particolarmente rigoroso in merito alla sorte processuale degli atti di indagine lesivi delle libertà fondamentali tutelate dalla Convenzione. Stando a un consolidato indirizzo pretorio, infatti, la mera violazione dell'art. 8 CEDU non produce alcun effetto invalidante dell'attività probatoria, occorrendo, a tal fine, anche una lesione del *fairness* processuale tutelato all'art. 6 CEDU[340]. Da questo punto di vista, dunque, il semplice *vulnus* arrecato alla riservatezza non può essere invocato, di per sé, per giustificare meccanismi invalidanti del materiale probatorio raccolto in sede di indagine[341].

Al fine di sciogliere il dubbio interpretativo sul quale ci si interroga, perciò, occorre sottolineare come, a dispetto di quanto sostenuto dalla giurisprudenza di legittimità, né l'art. 189 c.p.p., né gli artt. 55 e 348 c.p.p. – constatata la genericità delle previsioni *ivi* contenute[342] – rappresentino una idonea base legale (riserva di legge) per limitare la riservatezza. Come si è già osservato, infatti, gli approdi della giurisprudenza di Strasburgo in relazione al contenuto dell'art. 8 CEDU impongono, alla luce dell'espressione «*in accordance with the law*», un determinato *standard* qualitativo del quadro legale: chiarezza nella forma espressiva, specificità nella previsione delle situazioni legittimanti l'intromissione e nella predisposizione di strumenti di controllo, libera accessibilità al dato normativo e indicazione specifica dei presupposti, delle condizioni e dei limiti di utilizzo, sono i parametri individuati dalla Corte per offrire garanzie adeguate ed effettive contro possibili abusi del potere pubblico (cd. *minimum safeguards*)[343].

Com'è evidente, però, il paradigma predisposto dall'art. 189 c.p.p. non soddisfa simili parametri, di talché la riserva di legge convenzionale risulta, nella sostanza, inattuata; da qui,

[340] Così facendo, i giudici europei sembrano operare una netta distinzione tra la semplice violazione della riservatezza (cioè, la violazione della legalità processuale) e la lesione dei diritti al "giusto processo": cfr., per tutte, Corte edu, 12 luglio 1988, *Schenk c. Svizzera*. Sul punto, v. A. CABIALE, *I limiti alla prova nella procedura penale europea*, Milano, 2019, p. 151-161, il quale evidenzia come, nella pratica quotidiana dei giudici europei, l'inosservanza dell'art. 8 CEDU non assuma alcun rilievo dal punto di vista probatorio in termini di inutilizzabilità del materiale acquisito. La Corte, infatti, appare restia a riconoscere una contestuale violazione degli artt. 6 e 8 della Convenzione. Critico rispetto all'approccio adottato sul punto dai giudici europei, A. CISTERNA, *Cedu e diritto alla* privacy, in A. Gaito (a cura di), *I principi europei del processo penale*, cit., p. 212, secondo cui «nel processo penale è pur possibile che il giudizio della Corte europea si possa concludere con l'affermazione dell'equità del processo interno e con la stigmatizzazione dell'uso di determinati mezzi di intrusione nella privatezza dell'imputato; ma certo è logico attendersi che l'abuso della *privacy* comporti una distorsione della decisione di colpevolezza».

[341] La tesi è sostenuta, ad es., da M. DANIELE, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen*., 2013, 367 ss., per il quale, a tutto concedere, la violazione dell'art. 8 potrebbe giustificare l'operatività di un criterio legale di valutazione, «finalizzato a stigmatizzare gli elementi conoscitivi raccolti dagli organi inquirenti in assenza delle garanzie richieste dalla Corte» (p. 374).

[342] C. CONTI, *Accertamento del fatto e inutilizzabilità*, cit., p. 164.

[343] Cfr. Corte edu, 26 aprile 1979, *Sunday Times c Regno Unito*; Corte edu, 2 agosto 1984, *Malone c. Regno Unito*, par. 67; Corte edu, 26 marzo 1987, *Leander c. Svezia*. Come ricorda A. CAMON, voce *captazione di immagini*, cit., p. 144, la "legge" cui si riferisce l'art. 8 CEDU «deve avere certe "qualità": essere chiara, precisa, dettagliata; imporre che la sorveglianza sia autorizzata da un'autorità indipendente; indicare la natura dei reati in relazione ai quali il controllo è possibile, le categorie di persone suscettibili di subirlo, la sa durata, la procedura da seguire per esaminare, utilizzare e conservare i dati, le circostanze in cui si può o si deve distruggerli».

in una prospettiva *de lege lata*, l'inutilizzabilità procedimentale del materiale acquisito mediante *cyberpatrolling*[344].

7.2 Alla ricerca della legalità perduta… o meglio, mai esistita

L'analisi condotta nei paragrafi precedenti ha messo in luce, a livello di legislazione nazionale, un macroscopico *deficit* di legalità nella (mancata) regolamentazione del *cyberpatrolling*, tanto nella fase di prevenzione (*intelligence* e prevenzione *stricto sensu*), come in quella di repressione[345]. Nel caso di specie, perciò, è la prassi (atipica) che crea la Regola.

Da questo punto di vista, debbono essere confermate in questa sede le considerazioni offerte da autorevole dottrina allorquando, all'indomani dell'entrata in vigore della legge con la quale il Parlamento italiano ratificò la Convenzione sul *cybercrime*[346], affermava che «lo stato attuale della normativa processuale italiana in tema di operazioni investigative è visibilmente inadeguato»[347]. Il *lawmaker*, infatti, pare aver abdicato alle proprie funzioni, affidando alla giurisprudenza l'arduo compito di stabilire se, come e quando nuove metodologie di indagine a contenuto tecnologico possono essere adoperate nel corso della fase preliminare. Così facendo, però, sembra essersi concretizzato il timore – avanzato dalla letteratura processualistica già nella metà degli anni '90 – di un «lento, ma deciso, evolversi del nostro sistema penale verso forme di intervento poliziesco […] svincolate da parametri legali»[348]. L'impiego diffuso delle tecniche *cyberpatrol*, a ben considerare, è la conferma più evidente di come «brandelli e scampoli di stato di polizia hanno continuato a sopravvivere alla promessa dello stato di diritto»[349]; un'"ideal tipo", quest'ultimo, nel quale la legittimazione dell'agire poliziale deve ritenersi ancorata al principio di stretta legalità.

Nell'andare alla ricerca di soluzioni che siano maggiormente in linea con i canoni costituzionali e convenzionali, occorre muovere, anzitutto, da una moderna concezione della *privacy* che sia capace di ricomprendere al proprio interno tutte quelle attività *online* relative

---

[344] Invero, non parrebbe poi irragionevole sostenere financo una vera e propria "inesistenza" del materiale acquisito mediante *social network mining*. Autorevole dottrina, benché con riguardo, più in generale, all'impiego di mezzi di ricerca della prova «dinamici» in grado di eseguire una «sorveglianza continuativa di determinati dispositivo informatici […], nonché [un] monitoraggio delle attività in rete compiute attraverso i medesimi», ha difatti sostenuto che queste «captazioni occulte e indiscriminate di tutti i dati contenuti negli spazi informatici delle persone […] non possiederebbero i requisiti minimi indispensabili per integrare lo schema normativo dei mezzi investigativi» (così, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 1904). Simili argomentazioni, a ben vedere, potrebbero forse essere spese anche con riguardo alle acquisizioni effettuate mediante *cyberpatrolling*.

[345] L. TEN HULSEN, *Open Sourcing Evidence From The Internet – The Protection of Privacy In Civilian Criminal Investigations Using OSINT (Opens-Source Intelligence)*, in *Amsterdam Law Forum*, 11 giugno 2020, p. 10, la quale sottolinea come in numerosi paesi l'utilizzo di tecniche di OSINT non supererebbe il test di legalità previsto all'art. 8 CEDU, auspicando, di riflesso, un intervento legislativo volto a consolidare la «*legal certainty and prevent arbitrariness in police work*».

[346] L. 18 marzo 2008, n. 48, con la quale il legislatore nazionale ha ratificato e dato esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica.

[347] R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, cit., p. 137.

[348] R. ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata*, cit., p. 591.

[349] M. PARAVINI, *La polizia, la sua riforma, la società aperta*, in D. Fondaroli (a cura di), *Nuove strategie di polizia per una "società aperta"*, Milano, 2011, p. 12, il quale ricorda come ciò che distingue lo Stato di polizia dallo Stato di diritto sia proprio «l'obbligo o meno della predeterminazione formale dell'agire dei poteri».

a dati e informazioni pubblicamente disponibili. Principio duttile, malleabile e in continua evoluzione, la riservatezza costituisce la stella polare di qualunque riflessione in materia, quantomeno muovendo dalla tesi, qui sostenuta, che un controllo non occasionale di quanto condiviso nei *social network* rischia di mettere a repentaglio quella ineliminabile e fondamentale componente "pubblica" di codesto diritto fondamentale.

In queste coordinate, appare imprescindibile un intervento legislativo atto a circoscrivere modi e garanzie per lo svolgimento del *cyberpatrolling* occulto e continuativo in fase *stricto sensu* investigativa. Sarebbe auspicabile, in tale direzione, escludere l'intervento autonomo delle forze dell'ordine, esigendo, per converso, un vaglio preventivo da parte dell'autorità giudiziaria che indichi i casi, i tempi e le ragioni a sostegno della necessità dell'ingerenza nella vita privata del bersaglio.

L'operazione – occorre essere onesti – è tutt'altro che agevole, non foss'altro perché la distinzione – a livello teorico, sufficientemente chiara – tra sorveglianza *una tantum* e controllo continuativo, diviene, in una prospettiva pratico-empirica, difficilmente percepibile[350].

Il legislatore tedesco, come si è visto, ha individuato un parametro temporale: osservazione ininterrotta superiore alle 24 ore o che si protrae per più di due giorni[351]. Per converso, alcune linee guida inglesi in tema di investigazioni penali nelle piattaforme digitali contemplano nel concetto di "sorveglianza ripetitiva" quelle attività di controllo che si estrinsecano in «più di due visite di un profilo *social*»[352] o, altre ancora, in «più di tre settimane, anche non consecutive»[353]. Una linea esegetica, quest'ultima, che sembra essere stata avallata anche dalla Corte di Strasburgo, allorquando i giudici hanno ravvisato un'ingerenza nella vita privata nel caso di una sorveglianza sistematica e segreta mediante l'uso di riprese audiovisive in spazi pubblici per un periodo di ventitré giorni[354]. Le stesse difficoltà applicative, peraltro, sono state colte dalla più recente giurisprudenza nordamericana nel già richiamato caso *Stati Uniti c. Jones*[355]. Nella *majority opinion*, i giudici hanno osservato come risulti assai complesso individuare, in concreto, una netta linea di demarcazione tra le differenti forme di monitoraggio, specie a fronte della diversa rilevanza assunta dai beni giuridici di volta in volta coinvolti (come, ad esempio, nel caso di un furto o di un

[350] Sottolinea la presenza di «*significant practical hurdles*» nell'individuare il limite temporale che dovrebbe distinguere una sorveglianza continuativa da una sorveglianza *una tantum*, M. BEDI, *Social Network, Government Surveillance, and the Fourth Amendament Mosaic Theory*, in *Boston University Law Review*, 2014, p. 1813, 1845.

[351] Anche secondo B. MUND, *Social Media Searches and the Resonable Expectation of Privacy*, cit., p. 262, gli agenti di polizia giudiziaria sarebbero legittimati a svolgere *motu proprio* attività di monitoraggio sui profili pubblici solo per «*few hours*».

[352] PRIVACY INTERNATIONAL, *Is your Local Authority looking at your Facebook likes?*, 2020, p. 10, al sito *www.privacyinternational.org* (trad. nostra).

[353] Blackburn with Darwen Borough Council, *Procedural Guide for the use of covert surveillance and covert human intelligence sources*, 2017, all'indirizzo *https://democracy.blackburn.gov.uk/Data/Executive%20Member%20Decisions/20180316/Agenda/Document%207.pdf* (trad. nostra).

[354] Corte edu, 18 ottobre 2016, *Vukota-bojić c. Svizzera*, par. 58, 59.

[355] *Stati Uniti c. Jones*, cit.

omicidio)[356]. In realtà, non sembra opportuno, per quanto qui rileva, ricorrere esclusivamente a un criterio che faccia leva sul tipo di reato oggetto di accertamento, giacché, indipendentemente dalla gravità, l'attività di *cyberpatrolling* continuativo è destinata a incidere, in ogni caso e in egual misura, sul diritto tutelato all'art. 8 CEDU. Ciò che rileva ai fini della violazione, infatti, è la circostanza che l'insieme dei dati raccolti consenta all'autorità pubblica di trarre precise conclusioni sulla vita privata della persona interessata.

Va considerata, altresì, in una prospettiva *de jure condendo*, la possibilità di introdurre, in relazione alla *social network surveillance* investigativa, un controllo preventivo a opera di un'autorità terza e indipendente.

Come si è visto, però, la necessità di garantire piena operatività alla riserva di giurisdizione non pare poter essere ricavata né dall'art. 15 Cost. – giacché il *cyberpatrolling* non incide sulla segretezza delle comunicazioni –, né, tantomeno, dall'art. 2 Cost., privo di ogni riferimento a un controllo da parte dell'autorità giurisdizionale (o giudiziaria)[357]. Il baricentro dell'analisi, dunque, pare doversi necessariamente trasferire sul piano sovranazionale e, più nel dettaglio, all'esegesi offerta dalla Corte di giustizia dell'Unione Europea e dalla Corte europea dei diritti dell'uomo in relazione, rispettivamente, agli artt. 7 e 8 della Carta di Nizza e all'art. 8 CEDU.

Da questo angolo di visuale, i recenti approdi della giurisprudenza di Lussemburgo in tema di *data recention* sembrerebbero giustificare, in via interpretativa, la necessità di un provvedimento autorizzativo da parte del giudice per le indagini preliminari tutte le volte in cui un mezzo di ricerca della prova incida sul diritto alla riservatezza in maniera tale da consentire all'autorità inquirente di conoscere e apprendere le abitudini di vita di un determinato soggetto. In quella sede, com'è noto, i giudici europei hanno sostenuto che l'attività investigativa diretta ad apprendere i cd. dati esterni alle comunicazioni – cioè, la data, l'ora, la durata e i destinatari delle chiamate effettuate, nonché i luoghi in cui le stesse sono avvenute – consente di ricostruire *ex post* le abitudini di vita quotidiana dell'utente, provocando così una grave intromissione nel diritto alla riservatezza[358]. Di conseguenza, la Corte, al fine di rendere effettivo il principio di proporzionalità e stretta necessità sancito dalla Direttiva 2002/58/CE e dagli artt. 7 e 8 della Carta di Nizza, ha stabilito che l'accesso da parte delle autorità nazionali ai dati relativi al traffico e all'ubicazione di un determinata utenza debba essere subordinato a un controllo preventivo da parte di un «giudice o di un'autorità amministrativa indipendente»[359]. A quest'ultimo proposito, i giudici europei hanno recentemente offerto un'interpretazione autentica della clausola *de qua*, affermando che il controllo *ex ante* esercitato da un giudice ovvero da un'autorità indipendente richiede

---

[356] Ci si è chiesti, ad esempio, «*how is a court to figure out when surveillance is prolonged? In the context os stored records, the analogous question might be: How much aggregation must occur before the Fourt Amendament is implicated?*» (così, C. SLOBOGIN, *Domesic Surveillance of Public Activities and Transactions with Third Parties: Melding European and American Approaches*, in D.D. Cole – F. Fabbrini – S. Schulhofer (a cura di), *Surveillance, Privacy and Trans-Atlantic Relations*, cit., p. 34).

[357] Sulla difficoltà (se non anche una vera e propria impossibilità) di estendere la "doppia riserva" prevista agli artt. 13 ss. Cost. anche all'art. 2 della Carta, v., in termini espliciti, P. BRONZO, *L'impiego de*l trojan horse *informatico nelle indagini penali*, in *Rivista italiana di scienze giuridiche*, 2019, p. 349.

[358] CGUE, 8 aprile 2014, *Digital Rights Ireland*, par. 34.

[359] CGUE, 8 aprile 2014, *Digital Rights Ireland*, cit., par. 62.

che tale organo sia in grado di garantire un giusto equilibrio tra gli interessi connessi alle necessità dell'indagine nell'ambito della lotta contro la criminalità e il diritto fondamentale al rispetto della vita privata. Il perseguimento di tale obiettivo – ad avviso della Corte – presuppone necessariamente che, qualora il controllo sia esercitato da un'entità indipendente, quest'ultima debba «godere di uno *status* che le permetta di agire nell'assolvimento dei propri compiti in modo obiettivo e imparziale», nonché in «posizione di neutralità nei confronti delle parti del procedimento penale»[360], a nulla rilevando che questi sia tenuto, in base alla legislazione interna di uno Stato membro, a ricercare elementi di prova anche a discarico dell'indagato. Evidente è l'approdo del discorso con riguardo all'ordinamento italiano: il pubblico ministero (e, men che meno, la polizia giudiziaria), ancorché "parte imparziale", non è un soggetto terzo e neutrale rispetto all'esito delle indagini e del processo.

Ebbene, se tali considerazioni valgono con riguardo ai tabulati telefonici – che, come detto, consentono di trarre precise conclusioni sulla vita privata di un individuo – non sembra peregrino affermare, parimenti, che anche le informazioni apprese all'esito di operazioni di *social network patrolling* costituiscano la base per stabilire il profilo delle persone oggetto dall'attività intrusiva. Volendo accogliere questa suggestione, perciò, è auspicabile che il legislatore attribuisca il potere di autorizzare lo svolgimento di attività di *cyber*-pattugliamento a un soggetto indipendente, imparziale, terzo e neutrale[361].

S'immagina, a questo punto, l'obiezione.

La tesi delle "garanzie processuali minime" – ricavata direttamente dalla cd. teoria delle sfere di matrice teutonica[362] – accolta dalla giurisprudenza di legittimità sin dalla nota pronuncia in tema di videoriprese[363], considera ammissibile un mezzo di ricerca della prova che realizzi una violazione tenue di un diritto fondamentale – cioè, che non incida sul "nocciolo duro" della garanzia – pur a fronte di un provvedimento autorizzativo del pubblico ministero debitamente motivato. Calato nel conteso in esame, questo *modus interpretandi* potrebbe essere invocato per sostenere l'adeguatezza di un *placet* dell'organo d'accusa, poiché l'operazione di indagine, pur lesiva della privatezza, è realizzata, in ogni caso, su dati pubblici e, dunque, su informazioni che, in fondo, non meritano una tutela parificata a contenuti segreti.

Un'impostazione di questo tipo, tuttavia, non sembra affatto convincente e, anzi, merita di essere rigettata con piena convinzione. L'idea che il grado di lesione di un diritto fondamentale possa essere modulato a seconda dell'intensità dell'ingerenza e che da ciò si pretenda di ricavare una più o meno intensa applicazione delle garanzie «rappresenta un'inaccettabile soluzione di compromesso […] perché in fondo nega il principio di

[360] Per le ultime citazioni, CGUE, 2 marzo 2021, *H.K.*, parr. 53, 54.

[361] Resta salva, in ogni caso, la possibilità per il legislatore di introdurre una procedura d'urgenza che consenta un intervento immediato del pubblico ministero, cui dovrebbe seguire una convalida successiva ad opera del g.i.p., secondo lo schema classico proprio della disciplina delle intercettazioni.

[362] …elaborata dalla Corte Federale tedesca: cfr. C. CONTI, *Sicurezza e riservatezza*, in *Dir. pen. proc.*, 2019, p. 1578.

[363] Cass., Sez. Un., 28 luglio 2006, n. 26795, cit.

sussunzione, e, con esso, il primato della legge»[364], perlomeno tutte le volte in cui la libertà in questione sia qualificata, in termini espliciti o impliciti, come inviolabile. Un carattere, quest'ultimo, che, pur non vietando *in toto* eventuali limitazioni quando ciò appare giustificato da legittime ragioni di persecuzione penale[365], non consente, per nessun motivo, una graduazione di tutele.

A conferma della necessità di un intervento giurisdizionale, peraltro, soccorre, ancora una volta, la recente proposta di modifica normativa che ha interessato l'ordinamento iberico. Il legislatore spagnolo, nel già citato progetto ALECRIM del 2020, ha espressamente incardinato il potere di disporre operazioni di sorveglianza e raccolta sistematica e continuativa di informazioni *open access* in capo al giudice istruttore. La scelta, pur tenendo conto delle differenze strutturali tra il modello iberico e quello italiano, potrebbe senz'altro essere coltivata anche in una prospettiva nazionale. Si andrebbe così rafforzando la funzione di garanzia tradizionalmente riconosciuta al giudice per le indagini preliminari. Tutto sommato, non v'è poi da stupirsi se a fronte di metodologie investigative altamente pervasive, la giurisprudenza europea e, auspicabilmente, il legislatore nazionale, si muovono nell'ottica di rafforzare il vaglio giurisdizionale «sulle iniziative degli organi della investigazione che attingono le libertà fondamentali dell'individuo sottoposto alle indagini»[366]. È questo, del resto, il compito di chi, terzo e imparziale, è chiamato a tutelare i diritti dell'indagato in quella fase che precede l'esercizio dell'azione punitiva.

8. L'acquisizione transfrontaliera delle informazioni pubblicamente disponibili nei *social-accounts*: i nuovi scenari della *jurisdiction to investigate*

L'esistenza di una nuova forma di criminalità digitale che travalica i confini nazionali – riflesso diretto della "globalizzazione giuridica"[367] – rappresenta, senza ombra di dubbio, una delle cause primarie della crisi del principio di territorialità statale che, dal XVI secolo in avanti, governa sia le regole in materia di legge penale sostanziale[368], sia quelle volte all'accertamento del fatto in campo processuale.

---

[364] F. CAPRIOLI, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, in L. Lupária – L. Marafioti – G. Paolozzi (a cura di), *Dimensione tecnologica e prova penale*, Torino, 2019, p. 48, il quale mette in luce l'essenza della tesi in esame e, con essa, la sua intima inconsistenza: «pensiamo all'acquisizione dei tabulati telefonici o alle registrazioni effettuate dall'interlocutore. Sono violazioni dell'art. 15? Chissà, forse sì, forse no, certamente non sono violazioni gravi come un'intercettazione telefonica, e allora ci possiamo accontentare del provvedimento del pubblico ministero. La *toilette* dell'esercizio pubblico è domicilio? NO, non è proprio un domicilio, però è qualcosa che gli assomiglia molto, e allora per la videosorveglianza bastano le "garanzie minime"».

[365] R. ORLANDI, *Esistono davvero diritti inviolabili?*, in V. Fanchiotti – M. Miraglia (a cura di), *Il contrasto alla criminalità organizzata. Contributi di studio*, Torino, 2016, p. 265.

[366] M. FERRAIOLI, *Il ruolo di «garante» del giudice per le indagini preliminari*, Padova, 2001, p. 95.

[367] Sul tema del cd. diritto globale, v. sul versante nazionale, S. CASSESE, *Il diritto globale. Giustizia e democrazia oltre lo Stato*, Torino, 2009; e, nella letteratura straniera, N. KRISCH, *Beyond Constitutionalism. The Pluralist Structure of Postnacional Law*, Oxford, 2010.

[368] La legge penale italiana, com'è noto, obbliga tutti coloro che si trovano sul territorio dello Stato, a prescindere dalla qualifica di cittadini, stranieri o apolidi (art. 6 c.p.). Sulla trasformazione del modo di intendere lo *ius puniendi* in un contesto globale, v. U. SIEBER, *Legal Order in a Global Word. The Development of a Fragmented System of National, International, and Privat Norms*, in A. Von Bogdandy – R. Wolfrum (a cura di), *Max Planck Yearbook of United Nations Law*, 2010, 4, p. 1 ss.

A quest'ultimo proposito, il principio *de quo*, considerato *ius cogens* nel diritto internazionale giacché manifestazione dell'eguaglianza fra Stati sovrani, si propone di limitare l'estensione della giurisdizione – e, dunque, l'individuazione del foro competente – alle sole attività delittuose i cui elementi costitutivi, la condotta o gli effetti si sono realizzati nel territorio dello Stato[369]. Nella ricerca della *ratio essendi*, la dottrina ha acutamente osservato come l'ordinamento nazionale, nell'esercizio del potere sovrano, è tendenzialmente indifferente rispetto a quei comportamenti illeciti «che offendono beni di un ambiente sociale diverso da quello nel quale lo Stato esprime la pretesa del pieno controllo della vita giuridica»[370].

L'avvento di *Internet*, però, sembra aver minato, in parte, le fondamenta di tale principio. Se, in passato, il compimento di condotte criminose era necessariamente legato alla corporalità della persona e delle cose che la circondavano, oggi, la possibilità di muoversi indisturbati nel cyberspazio offre nuove opportunità all'agire illecito. I "leoni da tastiera", comodamente seduti nel proprio salotto, sono in grado di realizzare offese a interessi giuridici volti a tutelare beni, persone o cose che si trovano ben al di là dei confini nazionali.

La crisi del canone di territorialità, però, non ha interessato solo il versante della giurisdizione *stricto sensu* intesa o cd. *jurisdiction to adjudicate* (cioè, esercizio del potere di *ius dicere*), bensì ha esteso i propri effetti anche alla cd. *jurisdiction to investigate*[371].

Nella concezione classica, come noto, il principio di sovranità limita lo svolgimento di un'attività penale investigativa entro i confini dell'ordinamento nel quale il delitto è stato presumibilmente commesso (ovverosia, nel territorio sottoposto al potere politico dello Stato al quale appartiene l'autorità perquirente), salvo l'attivazione di strumenti di cooperazione giudiziaria e di polizia.

Questo assunto, però, complice pure l'avvento di una prova informatica svincolata da uno specifico ambito territoriale, deve essere oggi profondamente rimeditato. La dispersione spaziale della condotta umana nell'era digitale e la dimensione transnazionale delle operazioni illecite, infatti, hanno comportato una diversa allocazione delle tracce, degli indizi e degli elementi di prova necessari per la ricostruzione del fatto di reato[372]; questi ultimi, infatti, si collocano in una realtà virtuale nella quale il potere sovrano dello Stato fatica ad affermarsi. Onde rendersi conto di ciò, è sufficiente considerare, a mero titolo di esempio, l'attività di ricerca di informazioni contenute nelle "nuvole digitali". Nel contesto

[369] Fin dal noto caso Lotus (7 settembre 1927), la Corte permanente di giustizia internazionale ha stabilito che la giurisdizione non può essere esercitata da uno Stato al di fuori dei propri confini. Cfr. anche R.M. PERKINS, *The Territorial Principle in Criminal Law*, in *Hastings Law Journal*, 1971, p. 1155, il quale ricorda come «*the territorial theory takes the position that criminal jurisdiction depends upon the place of perpetration. That is, the nation on whose territory the crime was committed has jurisdiction of the offense. It is a logical outgrowth of the conception of law enforcement as a means of keeping the peace*».

[370] F. DEAN, *Norma penale e territorio*, Milano, 1962, p. 17.

[371] La locuzione *jurisdiction to investigate* è stata recentemente utilizzata da una parte della dottrina internazionalistica, affiancandola ai tradizionali concetti di *jurisdiction to prescribe*, *jurisdiction to adjudicate* e *jurisdiction to enforce* con l'obiettivo di mettere in evidenza l'autonomia e la specialità della categoria *de qua* rispetto alle altre forme di esercizio della giurisdizione statale (D. SVANTESSON – F. GERRY, *Access to Extraterritorial Evidence: The Microsoft Cloud Case and Beyond*, in *Computer Law & Security Review*, 2015, p. 478 ss.).

[372] A.K. WOODS, *Against Data Exceptionalism*, in *Standfor Law Review*, 2016, p. 745.

delle *cloud investigations*, infatti, è estremamente complesso – se non, talvolta, financo impossibile – riuscire a individuare l'esatta collocazione territoriale del dato che si vuole acquisire, giacché quest'ultimo – per ragioni di natura tecnico-informatiche – è libero di fluttuare liberamente nel cyberspazio[373]. In tali ipotesi, l'autorità investigativa, specie a causa della cd. *loss of location*, è in grado di verificare solo se l'informazione alla quale intende accedere è ubicata in un *server* nazionale; in caso contrario, essa non è in condizione di conoscerne l'esatta collocazione[374].

8.1 L'art. 32, comma 1, lett. a), della Convenzione di Budapest sul crimine informatico: il concetto di "fonte pubblica" nelle ipotesi di *transborder access*

In queste coordinate teoriche, non pare dubitabile che il potere di svolgere attività investigative per delitti commessi entro i propri confini costituisca esercizio legittimo di sovranità, indipendentemente dalla circostanza che dette operazioni siano compiute nello spazio fisico o in quello digitale[375]. L'assunto si giustifica considerando che il concreto ed effettivo esercizio della giurisdizione statale presuppone l'espletamento di una qualche forma di *jurisdiction to enforce*, cioè la facoltà di ricercare gli elementi di prova necessari per addivenire a una pronuncia giudiziale. È per tale motivo, dunque, che l'accesso diretto a dati elettronici memorizzati su un *server* situato nel territorio di un altro Paese viene comunemente valutato in termini di violazione della sua integrità territoriale e, perciò, qualificato come un atto internazionale illecito[376], salvo che vi sia un titolo legittimante l'acquisizione e, cioè, una norma consuetudinaria, una disposizione convenzionale o un'autorizzazione *ad hoc*.

Alla luce di tali premesse, il problema del *transborder data access* impone all'interprete di individuare un giusto equilibrio tra due contrapposte esigenze: da un lato, l'interesse dello Stato-richiedente di esercitare il potere investigativo in maniera funzionale alla repressione dei reati (e, dunque, al mantenimento dell'ordine pubblico); dall'altro, la contrapposta necessità dello Stato-richiesto di mantenere intatta la propria sovranità.

---

[373] Tanto che né gli utenti che usufruiscono del servizio *cloud*, né gli stessi ISP sono in grado di sapere con precisione dove siano ubicati i dati in un determinato momento. Su questa caratteristica del *cloud*, cfr. P. DE FILIPPI – S. MCCARTHY, *Cloud Computing: Centralization and Data Sovereignity*, in *European Journal for Law and Technology*, 2012, p. 1 ss. Per un'analisi della tecnologia utilizzata dalle nuvole digitali e sulle cause della "perdita di localizzazione", v. W.K. HON – C. MILLARD, *Cloud Technologies and Services*, in M. Millard (a cura di), *Cloud Computing Law*, Oxford, 2013, p. 1 ss.; R. LEENES, *Who controls the cloud?*, *Revista de Internet, derecho y política*, 2010, 11, p. 1 ss.; I. WALDEN, *Accessing Data in the Cloud: the Long Arm of the Law Enforcement Agent*, in *Queen Mary School of Law Legal Studies Research*, 10 marzo 2015.

[374] Senza voler considerare, in aggiunta, come la questione sembri complicarsi ancor di più laddove gli organi inquirenti intendano acquisire i cd. dati poliglotti, ovverosia informazioni dotate del dono dell'ubiquità, poiché allocate contestualmente in più Stati.

[375] In questi termini, v. anche U. SIEBER – C.W NUEBERT, *Investigaciones transnacionales de crìmenes en el ciberspacio: retos a la sobranìa nacional*, in A. Nieto Martìn – B. Garcìa Moreno (a cura di), *Ius puniendi y Global Law. Hacia un dereho penal sin estado*, Valencia, 2019, p. 319, per i quali «*a efecto de la administracòn de la Justicia penal, las investigaciones conservan el caràcter de actividades proprias de un Estafo en concreto, incluso cuando los agentes estateles simplemente "patrullan" internet*».

[376] B.J. KOOPS – M. GOODWIN, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law*, in *Tilburg Law School Research paper*, 2014, 5, p. 64.

Nella ricerca di soluzioni-compromesso, il legislatore europeo sembra aver trovato un punto di equilibrio proprio nell'ambito dell'acquisizione transfrontaliera delle informazioni pubbliche (*publicly available*) presenti nelle piattaforme digitali.

Nel Capitolo III della Convenzione di Budapest sul *cybercrime*, gli Stati contraenti hanno individuato due ipotesi in cui l'accesso *extra*-confine a dati informatici contenuti in Rete non incide in alcun modo sul principio di territorialità. Mediante la previsione di «*permissive rules*»[377], cioè casi eccezionali nei quali l'apprensione transnazionale di informazioni non richiede l'assistenza reciproca fra Stati, i *conditores* sembrano aver sviluppato un sistema capace di bilanciare le summenzionate esigenze, dando vita a un nuovo modello di cooperazione che prescinde dalla collaborazione dell'ordinamento in cui i dati sono allocati. Trattasi del cd. accesso diretto o unilaterale[378].

Oltre al caso in cui una Parte può accedere o ricevere dati informatici situati in un altro Stato qualora vi sia «il consenso legale e volontario della persona legalmente autorizzata a divulgar[li]» (art. 32, comma 1, lett. b), viene in rilievo, per quanto interessa in questa sede, il contenuto della lett. a) della medesima disposizione, a mente del quale uno Stato contraente può, senza l'autorizzazione di un'altra Parte, «accedere ai dati informatici immagazzinati disponibili al pubblico (fonti aperte), senza avere riguardo al luogo geografico in cui si trovano tali dati».

La previsione normativa – pressoché ignorata dai commentatori[379] – presenta, a ben vedere, due profili di carattere problematico: il primo, sul fronte definitorio (*i*); il secondo, sul versante della disciplina *ivi* contenuta (*ii*).

Innanzitutto (*i*), va osservato come la disposizione si presenti in termini tautologici con riguardo all'individuazione del concetto di «dati informatici disponibili al pubblico (fonti aperte)». Si è già ricordato, d'altro canto, come né l'art. 32, né il relativo *report* esplicativo[380] indichino con precisione i parametri per valutare il carattere *open access* di un'informazione digitale. Per di più, l'utilizzo contestuale di differenti locuzioni – «*publicly available*» e «*open source*» –, dal significato apparentemente identico, sembra rendere ancora più complessa l'attività esegetica.

Indicazioni utili, peraltro, non sembrano pervenire neppure dalla lettura di altri documenti internazionali dedicati alla tematica *de qua*. La Sezione n. 49 del *Trans-Border Access to Stored Computer Data, Content Data, or Traffic Data* elaborata dal *Common Market for Eastern and Southern Africa* (COMESA)[381] stabilisce che «*a competent authority may*

---

[377] Così la definisce L. TOSONI, *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, in *Computer Law & Security Review*, 2018, p. 1210.

[378] Di un «modello di "nuovo" conio, stravagante rispetto ai tradizionali strumenti di cooperazione giudiziaria» che rappresenta «una sorta di "applicazione informatica" dell'inseguimento transfrontaliero di cui all'art. 41 della Convenzione per l'applicazione dell'accordo di *Shengen* (C.A.A.S.)» parla F. SIRACUSANO, *La prova informatica transnazionale*, cit., p. 181.

[379] V., ad es., B.J. KOOPS – M. GOODWIN, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation*, cit., p. 53, per il quale l'art. 32, comma 1, lett. a) della Convenzione non pone problemi di carattere interpretativo poiché «*in those situations* […] *the police — just as anyone else — can easily retrieve the data*».

[380] CONSIGLIO D'EUROPA, *Explanatory Report to the Convention on Cybercrime*, 23 novembre 2001, par. 294.

[381] COMMON MARKET FOR EASTERN AND SOUTHERN AFRICA, *Trans-Border Access to Stored Computer Data, Content Data, or Traffic Data*, 2011.

access publicly available (open source) stored computer data, content data, or traffic data regardless of where the data is located geographically», senza specificare alcunché in merito ai criteri per individuare l'oggetto di quelle "fonti pubbliche" cui si riferisce la disposizione. Altrettanto generico è il contenuto dell'art. 40, comma 1, della *Arab Convention on Combating Information Technology Offences*, nella parte in cui si limita a consentire l'accesso transfrontaliero alle «*information technology available to the public (open source), regardless of the geographical location of the information*»[382]. Sembra rivelarsi di scarsa utilità pure la lettura delle normative nazionali di quegli Stati membri che hanno implementato la Convenzione con riguardo al disposto dell'art. 32, comma 1, lett. a). Tanto l'art. 25, comma 1, lett. a), della legge portoghese n. 109/2009, quanto l'art. 65, comma 2, della legge rumena n. 161/2003, ad esempio, si limitano a stabilire che le autorità straniere possono avere accesso alle informazioni pubbliche presenti in Rete, pur in assenza di una preventiva autorizzazione da parte delle autorità locali. Niente è detto, però, in merito al concetto di *public sources*.

Al contrario, interessanti spunti di riflessione possono essere tratti dalla lettura della *Guidance Note # 3 Transborder Access to data* del dicembre 2014, redatta dal *Cybercrime Convention Committee* nell'ambito del monitoraggio circa lo stato di avanzamento e implementazione della Convenzione. Dopo aver rilevato che «*with the Article 32a […] no specific issues have been raised*», il comitato, nell'intento di fornire una sorta di interpretazione autentica del disposto normativo, precisa che le forze dell'ordine possono accedere liberamente a qualunque dato *open access* potendo, a tal fine, «registrarsi o abbonarsi per i servizi disponibili al pubblico»[383]. Un inciso, quest'ultimo, che parrebbe legittimare attività transfrontaliere di *open source analysis* con riguardo a tutte quelle piattaforme digitali per il cui utilizzo è richiesta una preventiva iscrizione (anche dietro corrispettivo di denaro[384]). Alla luce di ciò, è possibile interpretare l'art. 32, comma 1, lett. a) della Convenzione come comprensivo di tutti quei dati ai quali chiunque può accedere senza restrizioni, cioè dati pubblicati su siti *web*, tra i quali debbono ritenersi comprese anche quelle informazioni «pubblicamente visibili nelle piattaforme dei *social network*»[385].

8.2 La libera accessibilità ai dati *open source* ubicati in territorio straniero: profili critici dell'art. 234-*bis* c.p.p.

Con riguardo alla disciplina (*ii*) dettata dall'art. 32, comma 1, lett. a), va osservato, anzitutto, come vi sia un sostanziale allineamento a livello contenutistico tra la Convenzione di Budapest e le altre fonti internazionali poc'anzi richiamate: le autorità investigative – si afferma – possono accedere a dati *online* pubblicamente disponibili a prescindere dalla loro ubicazione geografica, pur a fronte di una mancata collaborazione dello Stato interessato.

[382] LEAGUE OF ARAB STATES, *Arab Convention on Combating Information Technology Offences*, 2010.

[383] Per le due ultime citazioni, CYBERCRIME CONVENTION COMMITTEE, *Guidance Note # 3 Transborder Access to data (Article 32)*, 3 dicembre 2014, p. 4.

[384] Nello stesso senso, v. anche B.J. KOOPS, *Police Investigations in Internet Open Source*, cit., p. 660.

[385] In questi termini esatti, U. SIEBER – C.W NUEBERT, *Investigaciones transnacionales de crìmenes en el ciberspacio*, cit., p. 332 (trad. nostra).

In assenza di indicazioni contenute nel *report* illustrativo, la *ratio legis* pare riconducibile all'idea per cui nel caso di acquisizione di informazioni immesse volontariamente nella Rete deve ritenersi esclusa qualunque frizione con il diritto alla riservatezza[386]. In tale circostanza, inoltre, l'ordinamento nel quale solo allocati i dati non avrebbe alcun interesse a esercitare il potere sovrano a tutela della libertà dei propri cittadini[387]. A quest'ultimo proposito, infatti, è stato sostenuto che l'acquisizione occulta non incide in alcun modo sul principio di territorialità, poiché il funzionario di polizia che acquisisce i dati non si trova "fisicamente" in suolo straniero[388].

La tesi, però, non appare pienamente convincente, non foss'altro perché muove da una concezione restrittiva e ormai superata del principio in discussione, postulando che quest'ultimo sia chiamato a operare solamente in quelle ipotesi in cui l'attività investigativa comporti un'intrusione "fisica" nel territorio dello Stato in cui si trovano i dati. I fautori dell'esegesi qui censurata, infatti, sostengono che l'apprensione di informazioni *open access* contenute in Rete non costituisca esercizio extraterritoriale della giurisdizione penale, poiché non provocherebbe alcun mutamento esteriormente percepibile nel territorio del Paese terzo, requisito necessario per qualificare come illecite dette attività transfrontaliere[389].

In realtà, nel diritto internazionale si è da tempo sottolineato come al fine di valutare la legittimità o meno di un'operazione investigativa *extra*-confine debba tenersi conto non tanto del luogo in cui la stessa è realizzata, bensì di quello in cui gli effetti sono stati prodotti[390]. Non può fondatamente sostenersi, dunque, che gli ordinamenti nazionali, tollerando l'utilizzo di *Internet* sul proprio territorio, abbiano di fatto legittimato l'apprensione dei dati pubblici *ivi* presenti da parte di autorità straniere[391]. Com'è stato osservato da autorevole dottrina internazionalistica, infatti, la natura *open* delle informazioni che circolano nel cyberspazio non è «in alcun modo idonea a influenzare la questione del

---

[386] In questo senso, S. SIGNORATO, *Le indagini digitali*, cit., p. 166. Aderisce pure A. MANGIARACINA, *Nuovi scenari nell'accesso transfrontaliero alla prova "elettronica"*, in V. Militello – A. Spena (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, cit., p. 436, per la quale «se un soggetto immette dati in un luogo pubblico o aperto al pubblico, accetta il rischio che questi possano essere utilizzati anche per finalità investigative».

[387] Per questa opinione, v. M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie*, cit., p. 1902, per il quale in tali ipotesi «viene meno la necessità di tutelare la sovranità di uno specifico Stato». Di indifferenza «rispetto al luogo geografico dove si trovano i dati» parla A. MANGIARACINA, *Nuovi scenari nell'accesso transfrontaliero alla prova "elettronica"*, cit., p. 436.

[388] N. SEITZ, *Transborder Search: A New Perspective in Law Enforcement?*, cit., p. 33-38.

[389] Sembra adottare questa impostazione F. CAJANI, *Le indagini informatiche per i reati di cyberterrorismo*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, cit., p. 1819, il quale esclude ogni problema in termini di giurisdizione in quanto, grazie a una «finestra magica», la polizia giudiziaria sarebbe in grado di accedere «con un semplice *click*, ad un luogo diverso da quello sul quale ha giurisdizione […] senza però calpestarne il terreno». Nella medesima prospettiva, peraltro, si collocano quegli A. che sostengono l'illegittimità di un accesso digitale transfrontaliero nel corso delle indagini penali solo a condizione che l'intrusione abbia cagionato danni materiali al sistema informatico dello Stato estero. Cfr., in senso giustamente critico rispetto a quest'ultima visione, G.M. RUOTOLO, *Il ruolo del consenso del sovrano territoriale nel* transborder data access *tra obblighi internazionali e norme interne di adattamento*, in *La comunità internazionale*, 2016, p. 192.

[390] U. SIEBER – C.-W. NEUBERT, *Transnational Criminal Investigations in Cyberspace: Challenges to national sovereignty*, in *Max Planck Yearbook of United Nations Law*, 2017, p. 257; J.-B. MAILLART, *The Limits of Subjective Territorial Jurisdiction in the context of Cybercrime*, in *ERA Forum*, 2019, p. 382.

[391] Concorde N. SEITZ, *Transborder Search: A New Perspective in Law Enforcement?*, cit., p. 34.

necessario rispetto della sovranità territoriale dello Stato»[392]. *Ad abundantiam*, va sottolineato come, anche qualora si dimostrasse questa supposta e teorica carenza di interesse da parte dello Stato "invaso", l'ordinamento manterrebbe comunque la legittima pretesa di proteggere le proprie infrastrutture informatiche e la genuinità degli altri dati *ivi* contenuti[393].

In un contesto globale e iperconnesso, pertanto, il principio di territorialità deve essere interpretato nel senso di vietare qualunque forma di intrusione straniera (quale un'operazione investigativa) realizzata nel perimetro nazionale, anche mediante operazioni che interferiscono in quella porzione di *cyberspazio* di pertinenza statale.

In proposito, è interessante notare, altresì, come la scelta del legislatore internazionale di garantire libero accesso ai dati *open access* sia stata giustificata alla luce del diritto consuetudinario. Secondo una certa corrente di pensiero[394], i numerosi atti normativi sopra richiamati, l'elevato numero di Stati firmatari della Convenzione di Budapest[395] e la loro sostanziale indifferenza rispetto al tema *de quo* costituirebbero la prova dell'affermarsi di una *consuetudo*. È noto, in effetti, che la ripetizione nel tempo di un determinato comportamento (*diuturnitas*) nella convinzione diffusa della sua doverosità morale, sociale e giuridica da parte di tutti i soggetti coinvolti (*opinio iuris ac necesitatis*) siano condizioni necessarie e sufficienti per l'instaurarsi di una consuetudine, unanimemente riconosciuta tra le fonti del diritto internazionale.

La tesi, per quanto originale, desta qualche perplessità.

In primo luogo, l'inerzia manifestata dalle Nazioni contraenti[396] potrebbe essere il sintomo di una semplice omissione dovuta alla mancata conoscenza di questo fenomeno o, ancora, di una forma di acquiescenza inconsapevole. D'altro canto, è lo stesso legislatore pattizio ad aver manifestato espressamente nel 2001 una certa difficoltà nel dettare un «regime completo e giuridicamente vincolante che regoli questo settore», proprio in ragione della «mancanza di esperienza concreta con situazioni di questo tipo»[397].

In secondo luogo, occorre considerare che la norma consuetudinaria alla quale si vorrebbe attribuire efficacia cogente dovrebbe necessariamente ricalcare il contenuto dell'art. 32, comma 1, lett. a) della Convenzione; una disposizione, quest'ultima, che pone non pochi dubbi di carattere interpretativo.

Innanzitutto, la previsione pattizia ricorre al termine «*access*» per indicare quell'attività investigativa che può essere legittimamente realizzata dalle autorità inquirenti dello Stato membro. La *littera legis*, dunque, sembrerebbe delimitare detta operazione alla mera

---

[392] G.M. RUOTOLO, *Il ruolo del consenso del sovrano territoriale nel* transborder data access, cit. p. 197.

[393] In questi termini, v., ancora, U. SIEBER – C.W NUEBERT, *Investigaciones transnacionales de crìmenes en el ciberspacio*, cit., p. 325.

[394] Per i dovuti richiami, v., nuovamente, U. SIEBER – C.W NUEBERT, *Investigaciones transnacionales de crìmenes en el ciberspacio*, cit., p. 332.

[395] Attualmente, 68 Stati membri.

[396] In realtà, P. DE HERT – F. VAN LEEUW, *Cybercrime Legislation in Belgium*, in E. Dirix – Y.-H. Leleu (a cura di), *The Belgian reports at the Congress of Washington of the International Academy of Comparative Law*, Bruxelles, 2011, p. 520, hanno messo in evidenza come la maggior parte degli Stati membri dell'UE «tendono a considerare una ricerca transfrontaliera sul *web* effettuata dalle autorità straniere senza autorizzazione delle autorità competenti come una violazione della loro sovranità e del diritto internazionale», anche qualora l'attività sia compiuta su dati accessibili senza dover esercitare poteri coercitivi (trad. nostra).

[397] CONSIGLIO D'EUROPA, *Explanatory Report to the Convention on Cybercrime*, cit., par. 293 (trad. nostra).

visualizzazione delle informazioni pubblicamente disponibili, escludendo implicitamente la possibilità di acquisirle e archiviarle in *database* collocati sul territorio nazionale. La conclusione parrebbe avallata anche dalla diversa formulazione impiegata dall'art. 32, comma 1, lett. b), che, nel delineare la seconda ipotesi tassativa di accesso unilaterale dettata dalla Convenzione (cioè, il caso in cui vi sia il consenso legale e volontario della persona autorizzata a divulgare i dati), si riferisce espressamente tanto all'«accesso» quanto alla «ricezione» delle informazioni immagazzinate in un altro Stato. Allo stesso modo, l'art. 19, comma 1, della Convenzione contempla espressamente due attività tra loro differenti («*search*» o «*access*»), al pari di quanto previsto al terzo comma della medesima disposizione («sequestrare o acquisire»).

Alla luce di ciò, sembrerebbe possibile affermare, facendo leva sulla regola interpretativa ricavabile dal brocardo *Ubi lex voluit dixit, ubi noluit tacuit*, che, se il legislatore avesse voluto legittimare attività ulteriori, oltre a quella del mero accesso, avrebbe dovuto prevederlo in maniera esplicita, così come statuito nelle altre ipotesi or ora richiamate.

Ciò nondimeno, questa lettura è stata criticata da una parte della dottrina. Muovendo da un'esegesi teleologica della *voluntas legis*, autorevoli commentatori hanno sottolineato come uno degli obiettivi perseguiti dai *conditores* fosse quello di snellire le procedure di accesso ai dati presenti in Rete, al fine di consentire un successivo utilizzo del materiale raccolto in sede processuale. In questa prospettiva, perciò, l'attribuzione alla polizia giudiziaria di una mera facoltà di accesso al dato informatico senza legittimarne la successiva apprensione – e, di conseguenza, escludendo una futura fruibilità *in iudicium* – appare in contrasto con la finalità perseguita dal legislatore sovranazionale[398]. Diversamente argomentando, infatti, andrebbe avallata la sostanziale inutilità dell'attività captativa, poiché la conoscenza del materiale visionato non sarebbe processualmente spendibile.

Seguendo questa linea ermeneutica, pertanto, potrebbe sostenersi che l'art. 32, comma 1, lett. a) consenta alle autorità investigative tanto l'accesso al dato informatico *open access* collocato al di fuori del territorio nazionale, quanto la sua acquisizione per finalità *stricto sensu* procedimentali.

Se tale impostazione, in effetti, appare convincente, occorre sottolineare, però, come il suo accoglimento imponga di considerare i possibili *vulnus* che un'acquisizione massiva e continuativa di informazioni stanziate *ultra fines* può provocare sul versante del diritto alla riservatezza. Si è già avuto modo di sostenere, infatti, che il monitoraggio occulto e continuativo di dati pubblici – a differenza di una visione/acquisizione sporadica – realizzi un'attività lesiva del bene tutelato all'art. 8 CEDU. Sulla scorta di tale considerazione, dunque, sembra potersi affermare che, qualora l'autorità procedente non si limiti alla mera

[398] Così, U. SIEBER – C.W NUEBERT, *Investigaciones transnacionales de crìmenes en el ciberspacio*, cit., p. 334. A tal proposito, è stato osservato, altresì, che «*the term 'access' in paragraph (a) would seem to imply that authorities can also copy the data, even though the Convention usually distinguishes between accessing and copying data.30 But art. 32(a) and 32(b) are functionally equivalent in the object of acquiring data (while differing in the source of data and means of acquisition), and since art. 32(b) talks of 'access or receive' the data through a third person, with 'receive' implying that (a copy of) the data are provided, one can interpret art. 32(a) to imply that authorities can 'get hold of' the data by copying them after access*» (così, B.J. KOOPS, *Police Investigations in Internet Open Source*, cit., p. 658).

visualizzazione del contenuto *online* ubicato oltre confine, ma intenda procedere con un atto acquisitivo, l'operazione svolta pregiudichi la *privacy* del soggetto bersaglio.

Qualora si accolga detta prospettiva, parrebbe doversi rimeditare il giudizio positivo (e senza riserve) generalmente manifestato dalla dottrina italiana in relazione al disposto dell'art. 234-*bis* c.p.p. che rappresenta, in certo qual modo, la traduzione normativa a livello nazionale del contenuto precettivo previsto all'art. 32 della Convenzione.

La disposizione, introdotta in sede di conversione del d.lgs. 18 febbraio 2015, n. 7[399], si inserisce nel contesto della lotta al fenomeno terroristico, per il contrasto del quale il legislatore ha avvertito la necessità di introdurre strumenti investigativi *ultra fines*, consentendo alle autorità investigative di accedere "virtualmente" a dati informatici collocati sul territorio straniero. Nelle intenzioni del legislatore, il congegno avrebbe dovuto far fronte alla situazione di straordinaria necessità e urgenza che, «anche alla luce dei […] gravissimi episodi verificatisi all'estero», imponeva di perfezionare strumenti di prevenzione del fenomeno dei cd. *foreign fighters*, al fine di contrastare le attività di proselitismo a mezzo *Internet*, con l'ulteriore obiettivo di rafforzare l'attività del Sistema di informazione per la Sicurezza della Repubblica[400].

L'innesto normativo, passato quasi sotto silenzio, consente all'autorità procedente (e, dunque, alla stessa polizia giudiziaria *motu proprio*) di acquisire «sempre […] documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare».

Come risulta chiaro già da una prima lettura, la disposizione appare redatta in termini tanto generici da consentire di qualificare il nuovo e inedito mezzo di ricerca della prova come uno strumento a vocazione "ultrattiva", consentendone, *de facto*, un'applicazione ad ampio raggio con riguardo a qualunque ipotesi delittuosa, senza limitarne l'operatività al contesto delle indagini relative a reati di terrorismo internazionale, né, tantomeno, di criminalità informatica, contrariamente a quanto previsto dalla corrispettiva previsione di rango convenzionale (art. 32)[401].

Perdi più, il costrutto normativo – a differenza, ad esempio, della disciplina portoghese sopra richiamata – non sembra brillare certo per chiarezza espositiva e intellegibilità, tanto che taluni commentatori hanno affermato come non sia «affatto semplice comprendere né la sua utilità effettiva né tantomeno il suo reale ambito applicativo»[402]. A prima vista, infatti, l'unica ipotesi di *direct transnational access* presa in espressa considerazione è quella prevista nella lett. b) dell'art. 32 della Convenzione, cioè il caso di un accesso a dati non

[399] Art. 2, comma 1-*bis*), d.l. 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla l. 17 aprile 2015, n. 43.

[400] Così è dato leggere nell'*incipit* del d.l. 7/2015.

[401] Concordi, sul punto, S. ATERNO, *L'acquisizione dei dati personali tra misure antiterrorismo e intromissioni nella* privacy, cit., p. 165; L.V. BERRUTI, Cyber terrorism*: esigenze di tutela preventiva e nuovi strumenti di contrasto*, in *Leg. pen.* web, 15 gennaio 2016, p. 1; R. CANTONE, sub *Art. 234-bis c.p.p.*, in G. Canzio – R. Brichetti (a cura di), *Codice di procedura penale*, Milano, 2017, p. 1601; S. SIGNORATO, sub *Art. 234-bis c.p.p.*, in G. Illuminati – L. Giuliani (a cura di), *Commentario breve al Codice di procedura penale*, Milano, 2020, p. 989.

[402] R. CANTONE, sub *Art. 234-bis c.p.p.*, cit., p. 1601. Anche G.M. RUOTOLO, *Il ruolo del consenso del sovrano territoriale nel* transborder data access, cit. p. 196, ritiene che «la formulazione della norma lascia non poco perplessi».

liberamente fruibili. In questa circostanza, l'art. 234-*bis* c.p.p. consente l'acquisizione solo «previo consenso […] del legittimo titolare»[403].

In realtà, la disposizione, seppur implicitamente, sembra legittimare l'organo d'accusa ad acquisire *ad libitum* e *sine die*, per finalità di indagine, «dati informatici […] disponibili al pubblico», senza un consenso previo da parte dello Stato-investigato; e non v'è motivo di dubitare che, tra questi, possano essere annoverate anche quelle informazioni *open access*, foto, *post* e messaggi in chiaro pubblicati sui *social network*[404]. Il tenore letterale dell'ordito normativo, dunque, pare indirettamente autorizzare un'apprensione massiva e continuativa di dati *publicly available* ubicati in territorio straniero, per giunta omettendo ogni riferimento alle necessarie cautele da adottare al fine di garantire la non alterabilità del contenuto informativo[405]. Una soluzione, quest'ultima, che finisce per legittimare una sorta di «universalità della *jurisdiction to investigate* italiana del tutto priva di titolo

[403] Il concetto di «legittimo titolare», secondo l'opinione dominante in dottrina, non potrebbe essere identificato con chi si limiti a detenere i dati altrui (si pensi agli *internet provider* o ai *social network*), poiché diversamente «si rischierebbe di subordinare le attività istruttorie a logiche di natura privatistica» (così, M. DANIELE, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, cit., p. 836, nt. 40. Concorde, A. MANGIARACINA, *Nuovi scenari nell'accesso transfrontaliero alla prova "elettronica"*, cit., p. 435, nt. 47. Nello stesso senso, v. già, D. NEGRI, *La regressione della procedura penale ad arnese poliziesco*, cit., p. 54). Allo stesso tempo, l'espressione *de qua* non potrebbe essere riferita neppure al soggetto che ha formato i dati (nella maggior parte dei casi, lo stesso indagato), poiché, così operando, la disposizione sarebbe destinata a rimanere *in the book*, «potendosi verosimilmente ipotizzare che il consenso venga prestato solo per le acquisizioni *in favor*» (così, L.V. BERRUTI, Cyber terrorism*: esigenze di tutela preventiva e nuovi strumenti di contrasto*, cit., p. 4. Nello stesso senso, M. PITTIRUTI, Digital evidence *e procedimento penale*, cit., p. 29, nt. 111).

Questa impostazione, però, è stata recentemente sconfessata dalla Corte di cassazione, per la quale l'espressione *de qua* deve intendersi come riferita alla «persona giuridica che di quei documenti o di quei dati poteva disporre in forza di un legittimo titolo secondo l'ordinamento giuridico del paese estero, identificabile non soltanto nella persona fisica e/o giuridica che procede alla trasmissione e alla conservazione dei dati, ma anche nella polizia giudiziaria, nell'autorità giudiziaria, nella persona offesa, nell'amministrazione pubblica, nella società che gestisce il servizio telefonico, nell'*internet service provider*» (così, Cass. pen., Sez. I, 13 ottobre 2022, n. 6363, par. 1.3). Se così fosse, si potrebbe porre un problema di sovrapponibilità tra questa disciplina e il nuovo Regolamento (UE) 2023/1543 del Parlamento Europeo e del Consiglio del 12 luglio 2023 relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali. L'inedito apparato normativo, infatti, istituisce un meccanismo di collaborazione diretta tra autorità giudiziaria e *service provider*, procedimentalizzando in tal modo un *iter* per la formazione delle prove digitali transnazionali. È evidente, dunque, che, laddove si ritenga che l'espressione "legittimo titolare" possa identificarsi pure con il gestore privato delle piattaforme, occorrerebbe stabilire se, a fronte della necessità di acquisire un dato informatico all'estero, debba impiegarsi l'art. 234-*bis* c.p.p. ovvero la regolamentazione predisposta dal Regolamento europeo.

[404] Concorde S. ATERNO, *L'acquisizione dei dati personali tra misure antiterrorismo e intromissioni nella* privacy, cit., p. 165; ID., *Cloud Forensics: aspetti giuridici e tecnici*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, cit., p. 1964.

[405] All'indomani dell'entrata in vigore della disposizione, A. CISTERNA, *All'Aise l'attività di informazione verso l'estero*, in *Guida dir*., 2015, 19, p. 95, osservava quanto segue: «resta da considerare se tali procedure di acquisizione di questo materiale debbano osservare gli *standard* che, nel nostro ordinamento, sono fissati dagli articoli 254-*bis* e 352, comma 1-*bis*, del c.p.p. per le acquisizioni "informatiche, telematiche e di telecomunicazione", tra le quali figurano le garanzie di conformità agli originali e quella di immodificabilità del dato». Critici rispetto all'impossibilità di verificare se il materiale appreso in base alla procedura prevista all'art. 234-*bis* c.p.p. sia effettivamente rispondente a quello custodito pressi i *server* localizzati all'estero, R. DEL COCO, *L'utilizzo probatorio dei dati* whatsapp *tra lacune normative e avanguardie giurisprudenziali*, in *Proc. pen. giust.*, 2018, p. 536; M. PITTIRUTI, Digital evidence *e procedimento penale*, cit., p. 30; S. SIGNORATO, sub *Art. 234-bis c.p.p.*, cit., p. 989.

nell'ordinamento internazionale»[406] e in aperto contrasto con i più volte richiamati *dicta* della giurisprudenza europea in materia di tutela della riservatezza nei luoghi pubblici.

[406] Così, testualmente, G.M. RUOTOLO, *Il ruolo del consenso del sovrano territoriale nel* transborder data access, cit. p. 196.

CAPITOLO III

LE INVESTIGAZIONI *OPEN ACCESS* NEL SISTEMA DELLA CORTE PENALE INTERNAZIONALE

SOMMARIO: 1. La "trasfigurazione digitale" delle *investigations* per l'accertamento dei crimini internazionali: dalla prova testimoniale alla *open source evidence*. – 2. Il cd. *overblocking* e le implicazioni processuali legate alla rimozione dei contenuti *online*. – 3. "Metamorfosi soggettiva" delle indagini nel quadro della ICC: *web sleuthing* e *user-generated content* (cenni). – 4. La fase di ricerca della prova dinnanzi alla ICC. – 4.1 Verso una certificazione preventiva della *open source evidence*? – 4.2 *Discovery* e prova *social*: un binomio complesso. – 5. La fase giudiziale: ammissione e valutazione della prova

1. La "trasfigurazione digitale" delle *investigations* per l'accertamento dei crimini internazionali: dalla prova testimoniale alla *open source evidence*

Lo svolgimento delle indagini preliminari nell'ambito del procedimento dinnanzi alla Corte penale internazionale (*International Criminal Court*, ICC) è tradizionalmente affetto da numerose criticità, specialmente con riguardo alle attività di ricerca e apprensione delle fonti di prova, tanto documentali, quanto dichiarative[1].

Tali difficoltà possono essere ricondotte a un duplice ordine di ragioni.

Per un verso, la natura dei crimini per i quali si procede (art. 5 dello Statuto della ICC, d'ora in poi St. ICC[2]) rende evidente come le operazioni investigative siano destinate a svolgersi perlopiù in luoghi fisicamente poco accessibili, a causa di limitazioni dovute a motivi di sicurezza, diplomatici o logistici. Si tratta, generalmente, di Paesi caratterizzati da profonde instabilità politiche e sociali, territori dilaniati da guerre civili o lotte intestine tra fazioni rivali. Senza voler considerare, in aggiunta, come lo stesso "potere costituto" tenda a ostacolare l'accesso al materiale informativo, negando al *prosecutor* e ai suoi delegati l'ingresso nei territori dello Stato coinvolto[3]. A differenza di quanto è dato riscontrare negli ordinamenti nazionali (nei quali l'autorità può accedere fisicamente ai luoghi o, comunque, avere un contatto diretto con le fonti dichiarative), nell'ambito dell'accertamento dei crimini di competenza della ICC, il pubblico ministero – qualora non vi sia la collaborazione dello Stato interessato[4] – difficilmente potrà condurre indagini efficaci ed effettive.

---

[1] Il tema delle *investigations* nel contesto della ICC è stato scandagliato a fondo dalla dottrina. In generale, e per ulteriori riferimenti bibliografici, v. M. MIRAGLIA, *Diritto di difesa e giustizia penale internazionale*, Torino, 2011, p. 10 ss.; W.A. SCHABAS, *An Introducion to the Internatinal Criminal Court*, Cambridge, 2017, p. 232-282.

[2] Trattasi, com'è noto, dei «*most seriouse crimes of concern to the international community as a whole*», ovverosia genocidio, crimini contro l'umanità, crimini di guerra e di aggressione.

[3] L. FREEMAN – R. VAZQUEZ LLORENTE, *Finding the Signal in the Noise. International Criminal Evidence and Procedure in the Digital Age*, in *Journal of International Criminal Justice*, 2021, p. 175.

[4] In linea di principio, le investigazioni svolte nell'ambito della ICC devono essere condotte dalle autorità dello Stato interessato. Non mancano, tuttavia, casi nei quali il personale dell'ufficio del pubblico ministero, grazie ad accordi stipulati con le autorità nazionali, si è installato sul territorio dello Stato coinvolto per svolgere più efficacemente le indagini. Sul punto, v., anche per alcune esemplificazioni, W.A. SCHABAS, *The International Criminal Court. A Commentary on the Rome Statute*, Oxford, 2016, p. 852.

Per altro verso, il costante clima di tensione e i timori di future ritorsioni provocano tendenzialmente una certa ritrosia, o financo un netto rifiuto, nel rendere dichiarazioni testimoniali, tanto in sede di indagine, quanto in sede dibattimentale[5]: «*in court, as in war, witnesses bear the risck*»[6].

Nel corso degli ultimi anni, però, il panorama è notevolmente mutato. La ragione di tale cambiamento pare essere riconducibile all'inarrestabile dilagare della *digital evidence*[7] e delle investigazioni a contenuto tecnologico[8] anche nel contesto dei procedimenti penali dinnanzi alla ICC. A tale ultimo proposito, un ruolo di primo piano dev'essere riconosciuto alle informazioni *open access* ricavate dall'analisi dei *social network* che, senza timore di smentita, assumono oggi una posizione dirimente, vuoi nella fase di prevenzione (e predizione)[9], vuoi nell'ambito delle *investigations*[10]. Nonostante la dottrina continentale appaia sostanzialmente silente sul punto, alcuni autori d'oltreoceano hanno recentemente messo in rilievo come la *social network evidence* correlata a fonti *open source* «*is*

[5] R.J. HAMILTON, *User-Generated Content*, in *Columbia Journal of Transnational Law*, 2018, p. 13.

[6] Assai icasticamente, K. HIATT, *Open Source Evidence on Trial*, in *Yale Law Journal Forum*, 2016, p. 323.

[7] Per un'accurata disamina dell'evoluzione del diritto delle prove nella giustizia penale internazionale, nonché sull'avvento della *digital evidence* in tale contesto, cfr., per un'ampia trattazione, L. FREEMAN, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, in *Fordham International Law Journal*, 2018, p. 283 ss. Cfr. anche A. ASHOURI – C. BOWERS – C. WARDEN, *An Overview of the Use of Digital Evidence in International Criminal Courts*, in *Digital Evidence and Electronic Signature Law Review*, 2014, p. 115 ss.; M. POBLET – J. KOLIEB, *Responding to Human Rights Abuses in the Digital Era: New Tools, Old Challenges*, in *Stanford Journal of International Law*, 2018, p. 277 ss.

[8] Come sottolinea A. KOENIG, *From 'Capture to Courtroom'. Collaboration and the Digital Documentation of International Crimes in Ukraine*, in *Journal of International Criminal Justice*, 2022, p. 831, «*traditional forms of fact-gathering are now supplemented by an international network of digital documenters*». A quest'ultimo proposito, difatti, sono stati recentemente pubblicati numerosi protocolli che delineano le *best practices* alle quali conformarsi per l'acquisizione, la conservazione e il successivo utilizzo processuale del materiale informatico raccolto. Cfr., ad esempio, le *Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals*, 2021.

[9] E. IRVING, *Suppressing Atrocity Speech on Social Media*, in *American Society of International Law*, 2019, p. 256 ss.; F. D'ALESSANDRA – K. SUTHERLAND, *The Promise and Challenges of New Actors and New Technologies in International Justice*, in *Journal of International Criminal Justice*, 2021, p. 15, i quali sottolineano come la «*OSINT (including social network and big data analysis) can assist with tracking the movement of individuals or groups […], or even the 'mood' of specific groups — sometimes being able to predict with amazing precision the outbreak and location of identity-based protests or other atrocity risk factors*».

[10] Sottolineano questo dato, pur con diverse accentuazioni, J.D. ARONSON, *The Utility of User-Generated Content in Human Rights Investigations*, in M.K. Land – J.D. Aronson (a cura di), *New Technologies for Human Rights Law and Practice*, Cambridge, 2018, p. 129: «*over the past decade, open source, user-generated content available on social media networks and the Internet has become an increasingly important source of data in human rights investigations*»; ID., *Mobile Phones, Social Media and Big Data in Human Rights Fact-Finding: Possibilities, Challenges, and Limitations*, in P. Alston – S. Knuckey (a cura di), *The Transformation of Human Rights Fact-Finding*, New York, 2016, p. 441 ss.; D. MURRAY – Y. MCDERMOTT – A. KOENIG, *Mapping the Use of Open Source Research in UN Human Rights Investigations*, in *Journal of Human Rights Practice*, 2022, p. 554 ss.; L. FREEMAN, *Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court*, in S. Dubberley – A. Koenig – D. Murray (a cura di), *Digital Witness Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, Oxford, 2020, p. 432 ss.; A. KOENING, *Open Source Evidence and Human Rights Cases: A Modern Social History*, in S. Dubberley – A. Koening – D. Murray (a cura di), Digital Witness, cit., p. 32 ss.; N. MEHANDRU – A. KOENIG, *Open Source Evidence and the International Criminal Court*, in *Harward Human Rights Journal*, 15 aprile 2019; E. HIGGINS, *A New Age of Open Source Investigation: International Examples*, in B. Akhgar – P.S. Bayler – F. Sampson (a cura di), *Open Source Intelligence Investigation*, cit., p. 189 ss.

revolutionizing the […] *prosecution of international crimes*»[11] e sia perciò destinata ad assumere «*a key role in future investigations*»[12]. E, in effetti, non mancano casi nei quali la ICC ha fatto ricorso a quella che potremmo definire la *social network open source evidence*: *Al Mahdi*[13], *Bemba*[14], *Al-Werfalli*[15], *Al Hassan*[16] e i numerosi procedimenti sorti a seguito del conflitto siriano[17], solo per fare alcuni esempi.

In un contesto di "democratizzazione delle informazioni", i cittadini che vivono in ambienti belligeranti hanno cominciato a raccontare le proprie storie e influenzare direttamente i processi di accertamento dei fatti, mediante la diffusione di elementi di prova "in diretta", nello stesso istante in cui le condotte illecite vengono realizzate. È possibile affermare, dunque, che nel XXI secolo "ogni guerra ha la sua piattaforma": mentre nei conflitti siriani e nel Myanmar è prevalso l'utilizzo di *media* più tradizionali (rispettivamente, *YouTube* e *Facebook*), *TikTok* ha assunto un ruolo di prim'ordine nel videoregistrare le atrocità perpetrate in Ucraina[18].

La proliferazione di questo "tipo" probatorio (nonché, tecnica investigativa) è legata, in primo luogo, alle notevoli difficoltà di acquisizione delle prove "sul campo". In territori caratterizzati da conflitti perenni, come si è detto, gli *user-generated content*[19] – ovverosia, le informazioni (immagini, commenti, video, etc.) che gli utenti dei *social network* pubblicano nella propria rete di contatti – costituiscono oggigiorno i principali elementi di prova a disposizione delle autorità investigative[20]. Se, in passato, si riteneva che la raccolta di materiale informativo, in questo ambito, fosse caratterizzata da un necessario «*in-person contact*»[21] con la fonte di prova, la *user-generated evidence* impone di rimeditare, in parte, tale *modus pensandi*.

La rapida diffusione di questo nuovo *investigative tool* può essere spiegata anche alla luce dei ridotti "costi di gestione". Trattandosi di contenuti virtuali generati direttamente dagli utenti (*rectius*, dalle persone, spesso le stesse vittime, che si trovano nei luoghi di conflitto), il *prosecutor* non ha più necessità di mettere in moto la macchina investigativa tradizionale, cui consegue un notevole risparmio sia in termini temporali che di risorse umane.

---

[11] Y. MCDERMOTT – A. KOENIG – D. MURRAY, *Open Source Information's. Blind Spot Human and Machine Bias in International Criminal Investigations*, in *Journal of International Criminal Justice*, 2021, p. 86.

[12] Y. MCDERMOTT – A. KOENIG – D. MURRAY, *Open Source Information's*, cit., p. 87.

[13] Trial Chamber, *Prosecutor vs Ahmad Al Faqi Al Mahdi, Final Decision*, 27 settembre 2016.

[14] Trail Chamber, *Prosecutor v. Bemba e altri, Decision on Prosecution Requests for Admission of Documentary Evidence*, 16 giugno 2015.

[15] Pre-Trial Chamber, *The Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli, Warrant of Arrest*, 15 agosto 2017

[16] Trial Chamber, *The Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud, Decision on Prosecution application submitting 63 open source exhibits into evidence*, 15 giugno 2021.

[17] Cfr. J. DEUTH – H. HABAL, T*he Syrian Archive: A Methodological Case Study of Open Source Investigation of State Crime Using Video Evidence From Social Media Platforms*, in *State Criminal Journal*, 2018, p. 46 ss.

[18] A. KOENIG, *From 'Capture to Courtroom'*, cit., p. 834.

[19] R.J. HAMILTON, *User-Generated Content*, cit., p. 1 ss.; C. GEORGE – J. SCERRI, *Web 2.0 and User-Generated Content: Legal Challenges in the New Frontier*, in *Journal of Information, Law and Technologies*, 2007, p. 4 ss.

[20] Il dato è rilevato anche da R.J. HAMILTON, *Social media Platforms in International Criminal Investigations*, in *Case Western Reserve Journal of Law*, 2020, p. 217.

[21] R.J. HAMILTON, *User-Generated Content*, cit., p. 11.

Nondimeno, ciò non deve indurre nell'errore di pensare che le indagini condotte basandosi sugli *user-generated content* siano "a costo zero"; occorre considerare, infatti, le spese – talvolta ingenti – per l'acquisto, la gestione e la manutenzione dei *software* e delle risorse digitali necessarie per elaborare e archiviare le informazioni raccolte in Rete o trasmesse al *prosecutor* direttamente dai naviganti del *web*[22].

Il terzo e ultimo elemento che ha senz'altro contribuito all'ascesa di questa nuova tecnica è la sensazione di maggiore sicurezza che aleggia attorno al dato digitale *open source* acquisito nei *social network*. In contesti di guerra, com'è noto, le prove tradizionali sono spesso alterate o rese inaccessibili dagli stessi autori del reato[23]. Da questo punto di vista, perciò, non stupisce che le *publicly available information* ricavate dalle piattaforme digitali siano state definite come prove a «oggettività relativa»[24]; un'espressione cui si è fatto ricorso per contrapporre queste ultime alla testimonianza che, specialmente nel contesto dei crimini di guerra, ha da sempre dovuto fare i conti con l'annoso problema della credibilità della fonte dichiarativa e la fragilità della percezione umana[25].

2. Il cd. *overblocking* e le implicazioni processuali legate alla rimozione dei contenuti *online*

Nel 2017, numerose associazioni siriane per la tutela dei diritti umani pubblicarono sui *social network* alcuni video che mostravano le atrocità perpetrate nel corso della guerra civile. Per la prima volta nell'era di *Internet*, le prove di crimini contro l'umanità venivano diffuse sui tali piattaforme, tanto che si parlò, in proposito, del primo «*Youtube conflict in the same way that Vietnam was the first television conflict*»[26]. Sennonché, a distanza di poche ore dalla pubblicazione, i video furono inspiegabilmente rimossi. La causa è da rintracciare nelle peculiari *policy rules* adottate dalla *community* di *Facebook* – ma, ad oggi, generalmente in uso in tutti i *social network* – che obbligano il gestore della piattaforma a contrastare il fenomeno del terrorismo *online*, della pedopornografia, dell'*hate speech*, delle *fake news* e, in generale, dei cd. *extremist content*, cioè, contenuti pubblicamente visibili che non rispondono a quei canoni di "buona condotta digitale" enucleati dallo stesso ISP[27]. In

---

[22] Sottolinea questo aspetto, L. FREEMAN, *Digital Evidence and War Crimes Prosecutions*, cit., p. 175. Nello stesso senso, v. M. DE ARCOS TEJERIZO, *Digital Evidence and fair trial rights at the International Criminal Court*, in *Leiden Journal of International Law*, 2023, p. 9.

[23] Come rilevano Y. MCDERMOTT – A. KOENIG – D. MURRAY, *Open Source Information's*, cit., p. 87, «*the fact that this material can be obtained remotely also helps minimize the risk to witnesses: instead of asking an individual or individuals to testify to the relationship between alleged perpetrators, or the destruction of cultural property, or the alleged commission of crimes, for example, this may be shown through verifiable publicly available information*».

[24] Y. MCDERMOTT – A. KOENIG – D. MURRAY, *Open Source Information's*, cit., p. 87 (trad. nostra).

[25] Per tale motivo, alcuni autori hanno messo in luce come l'avvento di questa nuova tipologia probatoria possa minare il valore da sempre riconosciuto alla testimonianza, specialmente nel contesto della ICC (Y. MCDERMOTT – D. MURRAY – A. KOENIG, *Whose Stories Get Told, and by Whom? Representativeness in Open Source Human Rights Investigations*, in *www.opiniojuris.org*, 19 dicembre 2019).

[26] *https://www.fastcompany.com/40540411/erasing-history-youtubes-deletion-of-syria-war-videos-concerns-human-rights-groups*, ove si riprendono le parole pronunciate da Justin Kosslyn, *ex manager* di *Google*.

[27] L'*ex Chief privacy officer* di *Facebook*, Chris Kelly, ha espressamente dichiarato nel corso di un'intervista che «*we have devoted significant resources to developing innovative and complex systems to proactive monitor the site and its users*» per prevenire la diffusione di contenuti illeciti (*https://www.techmeme.com/090203/p73*).

quell'occasione, il fornitore del servizio informatico aveva sviluppato uno specifico algoritmo in grado di eliminare i video e i commenti riconducibili alla propaganda terroristica. Nel caso di specie, però, il *software* non era riuscito a distinguere tra i video postati in quel periodo dall'ISIS e quelli pubblicati dalle associazioni per i diritti umani.

Questo esempio, tra i molti[28], consente di mettere in luce uno degli aspetti maggiormente problematici legati all'utilizzo delle informazioni *open source* nell'ambito delle investigazioni penali internazionali.

Si allude, più nello specifico, al ruolo attribuito ai gestori privati delle piattaforme digitali. In questo contesto, l'interprete sembra essere chiamato a individuare un punto di equilibrio tra due contrapposte esigenze, entrambe meritevoli di seria considerazione.

Nell'intento di garantire uno "spazio virtuale" più sicuro nel quale i cibernauti possano svolgere le proprie attività di vita quotidiana, le società di *social media*, specie negli ultimi anni, hanno intensificato gli sforzi per rimuovere in modo permanente quei *post* pubblicati dagli utenti ritenuti in contrasto con le *policy* interne e le *community guidlines* a livello internazionale. Fino a poco tempo fa, l'operazione era realizzata perlopiù da personale formato *ad hoc* – i cd. moderatori di contenuti – che, di propria iniziativa o su segnalazione degli stessi utenti, provvedeva a eliminare tutte quelle notizie aventi natura illecita. Senonché, lo sviluppo dell'intelligenza artificiale ha consentito agli ISP di adottare un nuovo approccio, consistente nell'implementare l'uso di *software* di apprendimento automatico progettati per identificare e rimuovere i contenuti vietati. L'iniziativa è andata a buon fine: le statistiche più recenti messe a disposizione da *YouTub*e, ad esempio, mostrano come più del 90% delle informazioni illegali venga attualmente cancellato tramite l'impiego di algoritmi[29].

Dal punto di vista normativo, peraltro, va ricordato come gli ISP fossero già stati chiamati dal legislatore europeo a ricoprire il ruolo di vere e proprie "sentinelle digitali", con la precipua funzione di rimuovere tutti quei contenuti illeciti presenti nella porzione di *web* di loro competenza. L'art. 14, comma 1, lett. b) della Direttiva sul commercio elettronico[30], in particolare, attribuisce indirettamente al prestatore di un «servizio della società dell'informazione» – categoria nella quale, come si è visto, rientrano a pieno titolo anche i *Social network provider*[31] – la qualifica di "ausiliario delle forze di polizia", imponendo all'*host provider* di disabilitare l'accesso al pubblico alle *virtual information* di natura illecita. È in questo senso, del resto, che si è mosso pure il Parlamento tedesco – e non solo[32] – con la "Legge per il miglioramento dell'applicazione del diritto nei *social network*", entrata

---

[28] *https://about.fb.com/news/2018/11/myanmar-hria/*; h*ttps://www.amnesty.org/en/latest/news/2017/11/youtube-removals-threaten-evidence-and-the-people-that-provide-it/*.

[29] "Applicazione delle Norme della community di *YouTube*", periodo di riferimento ottobre-dicembre 2022, al sito *https://transparencyreport.google.com/youtube-policy/removals*.

[30] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.

[31] Cfr. Parte I, Cap. II.

[32] Anche in Austria, ad esempio, il legislatore ha adottato 1° aprile 2021 la *KoPL-G*, una regolamentazione *ad hoc* che ricalca i contenuti della disciplina tedesca.

in vigore il 1° ottobre 2017[33]. Il costrutto normativo, onde implementare, sulla scia del cd. *proxy censor*[34], strumenti diretti al contrasto dei crimini d'odio, impone agli ISP di istituire un sistema informatizzato di gestione dei reclami presentati dagli utenti, obbligando i primi a rimuovere, entro 24 ore dalla ricezione della doglianza, tutti quei contenuti qualificati come illegali dal paragrafo 1, comma 3, della legge. Sulla stessa linea di pensiero e nella consapevolezza della diffusione di «servizi nuovi e innovativi, quali le reti sociali (cosiddetti *social network*)», il Parlamento europeo ha recentemente approvato il 5 luglio 2022 il Regolamento sui servizi digitali (*Digital Service Act*[35]), il cui dichiarato obiettivo è, tra i molti, quello di imporre determinati obblighi di diligenza ai «prestatori di servizi intermediari per quanto riguarda il modo in cui dovrebbero contrastare i contenuti illegali, la disinformazione *online* e altri rischi per la società»[36]. Si attribuisce, dunque, agli ISP e, soprattutto, ai SNP, il compito di realizzare attività dirette all'individuazione, identificazione e rimozione/disabilitazione dei contenuti illegali presenti nel *web*[37]. Nel contesto dei crimini di guerra e contro l'umanità, questa funzione assume una particolare importanza, giacché consente di evitare che i video e le immagini rappresentanti le più efferate atrocità possano diffondersi in maniera incontrollata nella Rete. Come dimostrano numerosi studi scientifici, infatti, la visualizzazione ripetuta di simili contenuti rischia di assuefare la collettività a tali accadimenti, generando così una sorta di "desensibilizzazione sociale"[38].

Alla necessità di garantire che il cyberspazio divenga un luogo più sicuro nel quale ciascun cibernauta possa muoversi liberamente, si contrappone, però, sul versante investigativo, l'esigenza di tutelare la libera circolazione di quel materiale probatorio – specialmente, video e immagini – utile alla ricostruzione dei fatti. Di tutto ciò, peraltro, sembra essere cosciente lo stesso legislatore comunitario che, nel tentare di definire il concetto di "contenuti illeciti" nell'ambito del *Digital Service Act*[39], esclude espressamente «un video di un testimone

[33] Per un commento alla normativa, v. J. RINCEANU, V*erso una forma di polizia privata nello spazio digitale? L'inedito ruolo dei provider nella disciplina tedesca dei* social network, in *Sist. pen*., 11 marzo 2021.

[34] Trattasi di una forma di "censura per procura", cioè una modalità con la quale gli Stati nazionali affidano agli stessi gestori delle piattaforme il compito di filtrare i contenuti civilmente o penalmente illeciti pubblicati sul *web* dagli internauti (A. PAPA, *Espressione e diffusione del pensiero in* Internet. *Tutela dei diritti e progresso tecnologico*, Torino, 2009, p. 248-250).

[35] Regolamento del Parlamento europeo e del Consiglio 2022/2065 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), entrato in vigore il 25 agosto 2023. La citazione precedente è tratta dal Considerando n. 1 del predetto Regolamento.

[36] Regolamento del Parlamento europeo e del Consiglio 2022/2065, cit., considerando n. 2.

[37] Cfr., *amplius*, G. MORGESE, *Moderazione e rimozione dei contenuti illegali* online *nel diritto dell'UE*, in *Federalismi.it*, 12 gennaio 2022.

[38] Si vedano, sul punto, J.D. ARONSON, *The Utility of User-Generated Content in Human Rights Investigations*, cit., p. 129 ss.; C.B. ALI, *International Crimes in the Digital Age: Challenges and Opportunities Shaped by Social Media*, in *Groningen Journal of International Law*, 2021, p. 49. Occorre considerare, inoltre, che la mancata rimozione di tali contenuti potrebbe generare una responsabilità per omissione in capo agli stessi ISP. Su quest'ultimo aspetto, cfr., *amplius*, HUMAN RIGHTS COUNCIL, *Report of the indipendent international fact-finding mission on Myanmar*, 2018, par. 74; N. HAKIM, *How Social Media Companies Could Be Complicit in Incitement to Genocide*, in *Chicago Journal of International Law*, 2020, p. 83 ss.

[39] Cfr. Regolamento del Parlamento europeo e del Consiglio 2022/2065, cit., considerando n. 12, ove si afferma che «il concetto di "contenuto illegale" dovrebbe essere definito in senso lato per coprire anche le informazioni riguardanti i contenuti, i prodotti, i servizi e le attività illegali. Tale concetto dovrebbe, in particolare, intendersi riferito alle informazioni, indipendentemente dalla loro forma, che ai sensi del diritto applicabile sono di per sé illegali, quali l'illecito incitamento all'odio o i contenuti terroristici illegali e i contenuti discriminatori illegali, o che le norme applicabili rendono illegali in considerazione del fatto che

oculare di un potenziale reato», salvo che «la registrazione o la diffusione di tale video al pubblico non [sia] illegale ai sensi del diritto nazionale o dell'Unione»[40]. A fronte di tale quadro, accade frequentemente – come verificatosi nel caso libico richiamato *supra* – che gli ISP, nell'esercizio di una legittima e condivisibile funzione di "vigilanza virtuale" sui *damaged online content*, rimuovano, distruggano o cancellino involontariamente elementi di prova essenziali per la persecuzione dei crimini di guerra[41].

Al netto delle questioni concernenti la possibile menomazione della libertà di espressione derivante dall'attività di filtraggio (o censura?) realizzata dai gestori delle piattaforme[42], il tema, dal punto di vista processuale, è tutt'altro che irrilevante e impone di confrontarsi apertamente con il ruolo che vanno assumendo i gestori privati delle piattaforme nel corso delle "nuove" indagini penali internazionali. Com'è stato efficacemente osservato, «*relying on digital evidence also means relying on the platforms who host it*»[43].

In passato, il *prosecutor* era generalmente raffigurato come il *dominus* delle *investigations*. Gli artt. 53 ss. St. ICC affidavano – e affidano tutt'oggi – a un organo *super partes*[44] il potere-dovere di condurre le indagini, tenendo conto degli interessi e della situazione personale delle vittime e dei testimoni, nonché della natura del reato[45]. Ancorché tali previsioni siano formalmente in vigore, non può ignorarsi come elementi di prova fondamentali siano oggi nella disponibilità e nel controllo esclusivo di soggetti privati[46] che agiscono in base a *policies* e interessi di natura individuale, svincolati, perciò, da esigenze di giustizia e, specialmente, da quella pretesa «*to establish the truth*» che, incardinata nell'art. 54 St. ICC, costituisce (più o meno condivisibilmente) il valore guida delle indagini penali nell'ambito della ICC.

In questo contesto, la rimozione da parte dell'ISP di materiale processualmente rilevante può avvenire "a valle" o "a monte" della sua pubblicazione in Rete.

---

riguardano attività illegali. Tra queste figurano, a titolo illustrativo, la condivisione di immagini che ritraggono abusi sessuali su minori, la condivisione non consensuale illegale di immagini private, il *cyberstalking* (pedinamento informatico), la vendita di prodotti non conformi o contraffatti, la vendita di prodotti o la prestazione di servizi in violazione della normativa sulla tutela dei consumatori, l'utilizzo non autorizzato di materiale protetto dal diritto d'autore, l'offerta illegale di servizi ricettivi o la vendita illegale di animali vivi».

[40] Regolamento del Parlamento europeo e del Consiglio 2022/2065, cit., considerando n. 12.

[41] Su tale aspetto, v. F. D'ALESSANDRA – K. SUTHERLAND, *The Promise and Challenges of New Actors and New Technologies in International Justice*, cit., p. 23; R.J. HAMILTON, *Social media Platforms in International Criminal Investigations*, cit., p. 213 ss.; L. FREEMAN, *Digitally Disappeared: The Struggle to Preserve Social Media Evidence of Mass Atrocities*, in *Georgetown Journal of International Affairs*, 2022, p. 107, secondo la quale «*while removing terrorism-related content makes sense from a counterterrorism perspective, it causes problems for war crimes investigators and prosecutors who want to use it as evidence in criminal cases*».

[42] Per un approfondimento sul tema, cfr. A. PAPA, *Espressione e diffusione del pensiero in* Internet, cit., p. 241 ss.

[43] R.J. HAMILTON, *Social media Platforms in International Criminal Investigations*, cit., p. 223.

[44] L'art. 54, comma 1, lett. a), St. ICC, stabilisce che il pubblico ministero, al pari di quanto previsto all'art. 358 c.p.p. italiano, debba ricercare gli elementi di prova tanto a carico, quanto a discarico dell'indagato. Per tale ragione, l'organo d'accusa è stato definito da taluni commentatori come un «*officer of justice rather than a partisan advocate*» (così, W.A. SCHABAS, *The International Criminal Court*, cit., p. 849). *Contra*, M. MIRAGLIA, *Diritto di difesa e giustizia penale internazionale*, cit., p. 12, alla quale si rinvia per ulteriori considerazioni in merito al ruolo svolto dal *prosecutor* nel contesto della ICC.

[45] Art. 54, comma 1, lett. b), St. ICC.

[46] R.J. HAMILTON, *User-Generated Content*, cit., p. 5, la quale, in maniera lapidaria, afferma che «*now, ley aspect of investigations [in ICC] are increasingly undertaken by a range of private actors*».

Nel primo caso, il contenuto viene bloccato algoritmicamente prima della "messa in onda virtuale", cosicché nessuno, men che meno il *prosecutor*, è in grado di apprenderne il contenuto. Questo tipo di "cancellazione immediata", come dimostrano nuovamente le statistiche messe a disposizione da *YouTube*, è sempre più diffusa, tanto che circa il 40% del totale degli *user-generated content* rimossi dal *provider* nel 2022 non è stato neanche visualizzato dagli utenti, e più di un terzo ha ricevuto meno di dieci visualizzazioni[47].

Nel secondo caso, il problema non riguarda tanto l'astratta conoscibilità del dato – giacché il pubblico ministero ne ha una conoscenza immediata o, comunque, per il tramite di terzi –, bensì la possibilità di acquisirlo direttamente dal gestore della piattaforma, con garanzia circa la sua autenticità e genuinità. Com'è noto, infatti, l'acquisizione e la conservazione delle fonti digitali esigono particolari cautele onde evitare che il materiale acquisito possa essere alterato o modificato, pur involontariamente. Per tale ragione, queste attività devono essere realizzate nel rispetto di procedure standardizzate e in ossequio alle indicazioni contenute nelle numerose linee guida disponibili anche nel contesto internazionale.

Nella prassi, però, accade con una certa frequenza che il *prosecutor* non sia in grado di acquisire tempestivamente il materiale probatorio prima della sua rimozione, nel rispetto dei crismi sanciti dalle *best practices* elaborate in ambito tecnico-scientifico. Di conseguenza, l'accesso diretto al dato informatico custodito nei *server* dell'ISP rappresenta l'unico atto investigativo potenzialmente idoneo a garantirne una legittima apprensione e, di riflesso, la futura spendibilità processuale. In proposito, peraltro, non va trascurato il fatto che, perlomeno allo stato attuale, non è dato conoscere il tempo di archiviazione dei dati all'interno del *server* gestito dall'ISP, né se e dopo quanto tempo gli stessi vengano rimossi in via definitiva. Sennonché, *de lege lata*, lo Statuto della ICC non prevede una disciplina *ad hoc* che obblighi il gestore della piattaforma a condividere con l'autorità investigativa i dati da questa richiesti (e quelli eventualmente già rimossi). Mentre a livello europeo, le istituzioni governative (Consiglio, Commissione e Parlamento) hanno implementato strumenti di cooperazione che consentono un'acquisizione diretta della prova transfrontaliera[48], nel panorama internazionale il tema non sembra aver ricevuto l'attenzione che merita.

Alla luce di quanto osservato, un dato appare evidente: l'efficacia delle indagini penali nel contesto della ICC dipende (e dipenderà sempre di più) dalla capacità di tutti gli attori interessati di creare una qualche forma di collaborazione con i gestori delle piattaforme digitali. Non sono più immaginabili, in un quadro come quello attuale, indagini penali a trazione esclusivamente statale-pubblicista. Dati e informazioni processualmente rilevanti sono oggigiorno sotto il controllo di soggetti privati, e con essi occorre interloquire.

Una via astrattamente percorribile potrebbe essere quella di implementare meccanismi di conservazione delle prove di crimini di guerra, coinvolgendo direttamente i *providers*[49] o,

[47] "Applicazione delle Norme della community di *YouTube*", periodo di riferimento ottobre-dicembre 2022, cit.

[48] Sul tema, cfr., *amplius*, Parte II, Cap. V, par. 8.

[49] In tal senso, v. anche L. FREEMAN, *Digitally Disappeared: The Struggle to Preserve Social Media Evidence of Mass Atrocities*, cit., p. 110. In termini problematici rispetto a una simile proposta, v., però, F.

eventualmente, organizzazioni internazionali indipendenti, alle quali affidare il controllo degli archivi e la condivisione del materiale *ivi* conservato con l'autorità inquirente e le altre parti del procedimento.

Uno spunto in tal senso sembra pervenire dall'approvazione del recente Regolamento UE 2021/784[50] volto a contrastare la diffusione di contenuti terroristici *online*. La normativa comunitaria, per quel che interessa in questa sede, prevede un obbligo generale in capo al prestatore di servizi di *hosting* di conservare i contenuti terroristici – e i relativi metadati – rimossi, o il cui accesso è stato disabilitato, a seguito di un "ordine di rimozione" adottato da un'autorità competente (non necessariamente da identificarsi, *de iure condito*, in un organo giurisdizionale) individuata dal singolo Stato membro (art. 6)[51]. Ebbene, tra le finalità che legittimano questo dovere di *data collection*, il legislatore menziona espressamente la necessità di prevenire, indagare e accertare la commissione di reati in materia terroristica, mostrando così di essere pienamente consapevole dell'utilità investigativo-probatoria del materiale rimosso dal *web*. E che questa sia la via da percorrere è confermato pure dal d.lgs. 24 luglio 2023, n. 107 con il quale il Parlamento italiano ha adeguato la normativa nazionale alle disposizioni del Regolamento. Tra i numerosi obblighi imposti al *provider* spicca, difatti, quello di conservare, per finalità di contrasto al terrorismo, i contenuti rimossi o il cui accesso è stato disabilitato, in perfetta linea di continuità con il *dictum* dell'art. 6 del provvedimento europeo.

È in quest'ultima direzione, del resto, che sembrano muoversi i più accreditati e recenti progetti di ricerca a livello internazionale. Tra questi, merita di essere ricordata la *partnership*, inaugurata nel 2022 e promossa dalla *Blavatnik School of Government* dell'Università di Oxford, tra l'Oxford *Programme on International Peace and Security*, l'*International Bar Association* e l'*UC Berkeley Human Rights*[52], il cui obiettivo, sulla scorta delle linee guida elaborate dalla stessa Università di Berkeley (*Digital, Lockers: Options for Archiving Social Media Evidence of Atrocity Crimes*[53]), è quello di sviluppare modelli di cooperazione internazionale pubblico-privato che siano capaci di garantire un'efficace conservazione delle prove *open source* ricavate dalle piattaforme digitali.

D'ALESSANDRA – K. SUTHERLAND, *The Promise and Challenges of New Actors and New Technologies in International Justice*, cit., p. 32.

[50] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio del 29 aprile 2021 relativo al contrasto della diffusione di contenuti terroristici *online*. Per un commento, v. S. SIGNORATO, *Combating Terrorism on the Internet to Protect the Right to Life. The Regulation (EU) 2021/784 on Addressing the Dissemination of Terrorist Content Online*, in AA.VV., *Yearbook Human Rights Protection Right to Life*, Novi Sad, 2021, p. 403 ss. Nella letteratura straniera, si veda S.-F. RODRÍGUEZ RÍOS, *Una mirada al Reglamento (UE) 2021/784 como nuevo instrumento en la lucha contra la difusión del terrorismo en Internet*, in *Investigación penal en el siglo XXI: nuevas tecnologías y protección de datos*, diretto da S. Pereira Puigvert – F. Ordóñez Ponz, Cizur Menor, 2021, p. 339 ss.

[51] In ossequio al canone di proporzionalità, il periodo di conservazione, a mente dell'art. 6, comma 2, è pari a sei mesi dal momento della rimozione o della disabilitazione. Tuttavia, su richiesta dell'autorità competente o di un organo giurisdizionale, i contenuti terroristici possono essere conservati per un periodo ulteriore.

[52] *https://www.elac.ox.ac.uk/research/values-and-multilateralism-3/*.

[53] Human Rights Center. UC Berkeley School of Law Digital, *Lockers: Options for Archiving Social Media Evidence of Atrocity Crimes*, 2021, al sito *https://humanrights.berkeley.edu/sites/default/files/digital_lockers_report5.pdf*.

3. "Metamorfosi soggettiva" delle indagini nel quadro della ICC: *web sleuthing* e *user-generated content* (cenni)

In un fortunato libro del 2017, David Patrikarakos sottolinea come nel contesto dei crimini di guerra, «le persone sul campo che *twittano* foto […] sono diventate preziose, soprattutto perché spesso postano da zone troppo pericolose [e inaccessibili] per i giornalisti»[54] e per le stesse autorità investigative. In poche righe, l'Autore riesce a cogliere uno dei fenomeni più complessi nell'attuale quadro delle indagini penali internazionali. L'impiego massivo dei *social network* nel contesto della ICC ha provocato un ampliamento quantitativo (e qualitativo?) degli organi di indagine. Si vuol dire, cioè, che il *prosecutor* e i numerosi soggetti professionali che erano tradizionalmente deputati a condurre le *investigations* (agenti esperti, associazioni non governative, etc.) si trovano oggi affiancati – e, sotto certi aspetti, rimpiazzati – da nuove figure che, a seguito della "democratizzazione tecnologica", dispongono di artefatti (si legga, gli *smartphone*) in grado di "catturare" ogni istante di vita quotidiana.

Il riferimento corre, più nel dettaglio, ai cd. «*armchair sleuth*»[55] o «*detectives de sillòn*»[56]. Il fenomeno che si va descrivendo, invero, costituisce solo una delle numerose e complesse manifestazioni delle *civilian criminal investigations*, cioè la tendenza delle persone comuni a sostituirsi alle autorità pubbliche nello svolgimento di vere e proprie attività di indagine penale[57]. Non è un mistero, del resto, che i privati cittadini, grazie allo sviluppo delle nuove tecnologie dell'informazione, abbiano cominciato a realizzare operazioni di *web sleuthing* sui *social network*, consistenti nell'impiego di strumenti digitali che consentono a ciascun individuo di controllare le attività realizzate dai suoi simili, in una sorta di "vigilanza biunivoca".

Il mutamento di prospettiva rispetto al sistema tradizionale è così palpabile da non poter lasciare indifferente lo studioso del rito penale: il cittadino comune, da semplice testimone dei fatti, assume ora le vesti di un vero e proprio "agente privato di polizia". Com'è stato efficacemente osservato, il crescente coinvolgimento dei «*self-appointed vigilantes*»[58] nelle indagini penali è espressione di un radicale cambiamento nel *modus investigandi*: «*from professional and indipendent [agents], towards a more community focused security mechanism within a democratic participatory society*»[59].

L'importanza che vanno assumendo gli utenti del *web* in questo contesto, però, sembra andare ben oltre. Essi, come si è visto, non solo "creano" le prove, ma possono anche

---

[54] D. PATRIKARAKOS, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty–First Century*, Londra, 2017, p. 25.

[55] M. O'FLOINN – D. ORMEROD, *Social Networking Material as Criminal Evidence*, in *Criminal Law Review*, 2012, p. 506.

[56] A. RODRÍGUEZ ÁLVAREZ, *La «investigación viral»: una primera reflexión sobre el web sleuthing a partir del caso Gabby Petito*, in *Modernización, eficiencia y aceleración del proceso*, diretto da S. Pereira Puigvert – M.J. Pesqueira Zamora, Cizur Menor, 2022, p. 285.

[57] Una recente e accurata panoramica sul tema è offerta da L. TEN HULSEN, *Open Sourcing Evidence From The Internet*, cit., p. 1 ss.

[58] J.S. WILSON, *MySpcace, Your Space, or Our Space? New Frontiers in electronic Evidence*, in *Oregon Law Review*, 2007, p. 1227.

[59] L. TEN HULSEN, *Open Sourcing Evidence From The Internet*, cit., p. 12.

controllarle, alterale e, persino, cancellarle[60]. Da quest'angolo di visuale, *Internet* può divenire il veicolo per campagne di disinformazione che alterano la realtà dei fatti e possono indurre in errore il pubblico ministero e, di riflesso, il giudice. Non è poi così raro, d'altro canto, imbattersi in casi come quello che ha avuto ad oggetto la deportazione Rohingya in Myanmar. Le autorità investigative erano giunte in possesso di numerosi video pubblicati sui *social network* che mostravano le violenze perpetrate a danno del gruppo di minoranza etnica[61]. Niente di più falso[62]: «*in the post-truth word, the camera often lies*»[63].

Il problema, peraltro, sembra destinato ad accentuarsi con l'avvento di nuovi modelli di intelligenza artificiale, denominati *Generative Adversary Network*, che consentono di modificare, o creare *ex novo*, video e immagini pubblicate sui *social network*. Il fenomeno, noto come *deepfake*, rischia seriamente di pregiudicare l'attività di ricerca e raccolta delle prove[64], non foss'altro perché, in un contesto come quello in cui è chiamata a operare la ICC, gli interessi politici in gioco e la disponibilità di ingenti risorse finanziarie potrebbero determinare un impiego massiccio di notizie "profondamente false". A fronte di tale quadro, l'auspicio è che la Corte penale internazionale possa intraprendere quel percorso tracciato dai giudici Van den Wyngaert e Morrison nella *separate opinion* resa nel caso *Jean-Pierre Bemba Gombo*: in un'epoca in cui è sempre più difficile distinguere ciò che è vero da ciò che è falso, «*it is crucial that the judiciary can be relied upon to uphold the highest standards of quality, precision and accuracy* [*of evidence*]»[65].

4. La fase di ricerca della prova dinnanzi alla ICC

L'art. 54, comma 1, lett. f), St. ICC, stabilisce che il *prosecutor* debba adottare nel corso delle *investigations* tutte le misure necessarie per garantire la confidenzialità delle informazioni raccolte, la protezione dei possibili testimoni e, per quel che più interessa in questa sede, «la conservazione degli elementi di prova», in modo da garantirne l'accuratezza e la genuinità, ovverosia la futura spendibilità processuale. Nel contesto di una *social network evidence* basata su fonti aperte, in particolare, è interesse primario dello stesso

[60] C.B. ALI, *International Crimes in the Digital Age*, cit., p. 47.

[61] Un altro caso si è verificato in Siria nel 2014. In un video pubblicato sui *social network*, intitolato "*Syrian Hero Boy*", un giovane ragazzo veniva rappresentato nell'atto di liberare una fanciulla rimasta intrappolata durante una sparatoria. A distanza di tempo, però, è stato dimostrato che l'incidente era stato inscenato sul set del film (*https://www.bbc.com/news/blogs-trending-30057401*).

[62] *https://www.wired.com/story/opinion-the-world-needs-deepfake-experts-to-stem-this-chaos/*.

[63] F. D'ALESSANDRA – K. SUTHERLAND, *The Promise and Challenges of New Actors and New Technologies in International Justice*, cit., p. 24.

[64] Sui rischi derivanti dalla diffusione di *deepfake* nelle investigazioni per i crimini internazionali, v. R.J. HAMILTON, *Social media Platforms in International Criminal Investigations*, cit., p. 218; A. KOENING, *"Half the Truth is Often a Great Lie": Deep Fakes, Open Source Information, and International Criminal Law*, in *American Journal of International Law*, 19 agosto 2019; F. D'ALESSANDRA – K. SUTHERLAND, *The Promise and Challenges of New Actors and New Technologies in International Justice*, cit., p. 25. L. FREEMAN, *Law in Conflict. The Technological Transformation of War and its Consequences for the International Criminal Court*, in *International Law and Politics*, 2019, p. 859. È opportuno sottolineare come la manipolazione, in questi casi, può riguardare tanto il video in sé, quanto singoli aspetti collaterali (ad esempio, oggetti presenti, luogo, data, etc.). Cfr. anche Human Rights Center of Berkeley School of Law, *The New Forensics. Using Open Source Information to investigate Grave Crimes*, 1° luglio 2018, p. 9.

[65] Appeals Chamber, The Prosecutor v. Jean-Pierre Bemba Gombo, *Separate Opinion of Judge Van den Wyngaert and Judge Morrison*, 8 giugno 2018, par. 5.

pubblico ministero ottenere e archiviare dati accurati sui quali poter fondare le proprie determinazioni all'esito delle indagini.

In questa prospettiva, si rende necessario esaminare un duplice ordine di questioni.

4.1 Verso una certificazione preventiva della *open source evidence*?

Com'è noto, la *golden hour* delle investigazioni digitali è temporalmente limitata a causa della volatilità e manipolabilità dei dati informatici, specialmente qualora, come nel caso della *social network evidence*, questi siano allocati in un ambiente virtuale contraddistinto per la transitorietà delle informazioni *ivi* contenute, cioè per l'intrinseca capacità di diffondersi nel cyberspazio. Nell'ambito delle piattaforme digitali, come si è detto, gli *user-generated content* possono essere pubblicati, modificati, manipolati ed eliminati con estrema facilità. Dal punto di vista investigativo, pertanto, l'autorità procedente è chiamata a intervenire nel più breve tempo possibile; solo in tal modo, infatti, possono essere minimizzati i rischi che la prova vada dispersa o sia contaminata[66]. D'altro canto, a meno che il materiale raccolto non sia verificato nelle primissime fasi delle indagini, «*it will potentially be impossible to rely on it at trial*»[67].

Nella piena consapevolezza di tali problematiche, l'*Office of the United Nations High Commissioner for Human Rights* e l'Università della California hanno redatto nel 2022 un Protocollo sull'utilizzo delle *open source information* nel contesto delle indagini sulle violazioni del diritto penale internazionale[68]. Le linee guida, più in particolare, individuano i migliori *standards* tecnici e giuridici per condurre ricerche *online*, fornendo indicazioni sulle metodologie e sulle procedure per l'analisi e la conservazione dei dati.

Quasi contestualmente, numerose associazioni in difesa dei diritti umani, in collaborazione con imprese operanti nel settore dell'*hi-tech*, hanno investito ingenti risorse per la creazione di veri e propri «cittadini investigatori digitali»[69], fornendo loro strumentazioni e *guidelines* al fine di poter acquisire video e immagini (nonché, i relativi metadati) ed essere in grado di trasmetterli in maniera sicura ai *server* della compagnia[70]. *EyeWitness to Atrocities*, *Videre Est Credere* e *CameraV* sono solo alcuni esempi di come le nuove tecnologie siano capaci di offrire gratuitamente strumenti in grado acquisire le prove delle violazioni dei diritti umani in contesti di guerra.

L'esito proficuo di tali progetti è comprovato dall'interesse manifestato dallo stesso Ufficio del Procuratore presso la ICC che, in collaborazione con *Eurojust*, ha pubblicato alcune raccomandazioni per le «organizzazioni della società civile sulla documentazione dei

---

[66] Del resto, proprio la "tempestività" è uno dei caratteri fondamentali dell'attività di OSINT (G. COSTABILE, *Le indagini digitali*, cit., p. 85).

[67] F. D'ALESSANDRA – K. SUTHERLAND, *The Promise and Challenges of New Actors and New Technologies in International Justice*, cit., p. 26.

[68] Office of the United Nations High Commissioner for Human Rights, Human Rights Center at the University of California, Berkeley, *Protocol on Digital Open Source Investigations*, 2022, al sito *https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf*. Per una disamina dei contenuti specifici del protocollo, v. N. MEHANDRU – A. KOENIG, *ICTS, Social media & the Future of Human Rights*, in *Duke Law & Technology Review*, 2019, p. 139-144.

[69] Mutuando l'espressione di S. GREGORY, *Ubiquitous Witnesses: Who Creates the Evidence and the Live(d) Experience of Human Rights Violations?*, in *Information, Communication & Society*, 4 agosto 2015.

[70] *https://vae.witness.org/video-as-evidence-field-guide/*.

principali delitti internazionali», come i crimini di guerra e i crimini contro l'umanità[71]. Le *guidlines*, oltre a fornire un inquadramento generale della tematica, sembrano delineare un vero e proprio nuovo *modus investigandi*. Con riferimento, ad esempio, alle operazioni di *videotape*, si suggerisce alle autorità di «*record the day, time and location (WHEN and WHERE) of the images (with GPS coordinates where possible)*», nonché di configurare il «*device to record as much relevant metadata in relation to the captured images as possible*»[72].

Le numerose iniziative delle quali si è dato conto costituiscono un chiaro indice della tendenza, sviluppatasi a livello internazionale, di implementare l'impiego "strumenti privati" di ricerca della prova (*rectius*, gli *smartphone* e le nuove tecnologie dell'informazione) che siano in grado di acquisire e, contestualmente, certificare in tempo reale l'autenticità di un determinato contenuto pubblicamente disponibile in Rete.

Prendendo le mosse da tale inquadramento, perciò, non sembra peregrino interrogarsi circa la necessità di fornire alle autorità investigative artefatti in grado di coadiuvarne l'operato nelle prime battute delle indagini. Un approccio di questo tipo, a ben considerare, avrebbe il pregio di minimizzare il rischio di imbattersi in "fonti aperte" volontariamente manomesse, come tali in grado di sviare inconsapevolmente le investigazioni. Come si è detto, non può dubitarsi del fatto che tra le informazioni acquisibili nei *social network* vi siano anche video oggetto di falsificazione mediante *deepfake technologies*; anzi, i SNS costituiscono la sede privilegiata nella quale questa tipologia di "inganno digitale" può esplicare maggiormente i suoi effetti perversi.

Le predette considerazioni – lungi dal voler creare falsi allarmismi – consentono di mettere in luce la necessità di adottare approccio giuridico al fenomeno *de quo* che sia maggiormente in linea con l'attuale stato di avanzamento tecnologico. Numerose Corti americane, d'altro canto, hanno già messo in guardia dal rischio elevato di falsificazione della *social network evidence*, specialmente con riguardo ai *deepfakes*: «*in the age of fake social-media accounts, hacked accounts, and so-called deepfakes, a trial court faced with the question whether a social-media account is authentic must itself be mindful of these concerns*»[73]. Affidarsi, *sic et simpliciter*, alla percezione umana, dunque, potrebbe non essere più sufficiente, specialmente nel corso di quell'attività investigativa di "rastrellamento" dei *social network*: il sillogismo fonti aperte=fonti affidabili appare assai discutibile.

È in questa prospettiva, pertanto, che appare doveroso chiedersi se non sia giunto il momento di implementare strumenti normativi che valorizzino una certificazione preventiva di autenticità del materiale *open access* raccolto nel corso di attività investigative nella Rete. Le tecnologie attualmente disponibili (applicazioni e *software*), come ben evidenziano i documenti sopra richiamati, consentono oggi di attestare tempestivamente la genuinità delle

[71] *Documenting international crimes and human rights violations for accountability purposes: Guidelines for civil society organisations*, 21 settembre 2022, al sito *https://www.icc-cpi.int/news/icc-prosecutor-and-eurojust-launch-practical-guidelines-documenting-and-preserving-information.*

[72] *Documenting international crimes and human rights violations for accountability purposes*, cit., p. 28.

[73] *People vs. Smith*, 18 febbraio 2021, n. 346044.

informazioni estratte dalle piattaforme *social*, garantendone così la futura spendibilità processuale.

Invero, non è nuova l'idea di ricorrere ad artefatti in grado di certificare la provenienza e la non alterazione di un determinato contenuto *online*. L'ordinamento spagnolo, ad esempio, ha recentemente introdotto un sistema di attestazione preventiva mediante la predisposizione di un *software* (denominato *eGarante*) che permette di accreditare l'esistenza di contenuti virtuali. Come è dato leggere nella *official web-page* della *Guardia civil national*[74], lo strumento risulta particolarmente importante sia per le vittime che intendono denunciare delitti commessi in Rete, sia per accertare la genuinità delle informazioni *open access* raccolte sui *social network* e allegate agli atti di denuncia-querela. L'applicazione, più nel dettaglio, consente di certificare l'indirizzo *web* (URL), il suo contenuto, la data, l'ora di visualizzazione, etc., realizzando una sorta di fotografia istantanea e "in diretta" del dato digitale, così per come visualizzato dall'utente in quello specifico istante, inibendo in tal modo successive manipolazioni o alterazioni[75].

Si è ben consapevoli, tuttavia, che una simile operazione, benché funzionale allo svolgimento di *investigations* più efficienti, non è certo priva di rischi[76]. Nelle indagini penali internazionali, infatti, gli spazi di intervento riservati alla difesa sono assai ridotti a livello teorico e ancor più limitati nella prassi. Il timore, dunque, è che l'implementazione di meccanismi tecnico-normativi diretti alla certificazione preventiva del materiale raccolto possa far confluire nel *trial* prove "incontestabili", rispetto alle quali anche un contraddittorio postumo potrebbe rivelarsi di mera facciata e, perciò, ineffettivo.

4.2 *Discovery* e prova *social*: un binomio complesso

Un secondo ordine di problemi è destinato a manifestarsi con riguardo alla fase della *disclosure*. Com'è noto, l'ostensibilità del materiale probatorio raccolto dal *prosecutor* nel corso delle indagini preliminari si modella diversamente rispetto a quanto previsto nell'ordinamento italiano, trovando la sua prima realizzazione solo in vista della *confirmation hearing*[77] e limitatamente al materiale probatorio necessario per richiedere il rinvio a giudizio. In linea generale, l'art. 67, comma 1, lett. a) e b), St. ICC, cristallizza il diritto dell'indagato di conoscere, con sufficiente anticipo rispetto all'inizio del processo, gli elementi di prova sui quali il *prosecutor* intende fondare le proprie accuse, salvo che non si tratti di informazioni la cui diffusione potrebbe minare l'efficacia delle indagini o l'incolumità delle fonti dichiarative. Nella prassi, tuttavia, la facoltà di limitare l'accesso alla difesa del materiale probatorio è stata oggetto di un «uso smodato»[78] e talvolta

[74] *https://www.guardiacivil.es/en/prensa/historico_prensa/4981.html*.

[75] G. DELGADO MARTÍN, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 214.

[76] Si pensi alle problematiche concernenti la tutela della *privacy*. Il rischio concreto di un'alterazione delle prove induce spesso l'autorità investigativa «ad acquisire i contenuti in blocco prima di esaminarne la pertinenza», così L. FREEMAN, *Digital Evidence and War Crimes Prosecutions*, cit., p. 176 (trad. nostra).

[77] Trattasi «di un ibrido, tra udienza preliminare all'italiana e *preliminary hearing* di *common law*», nella quale, in contraddittorio tra le parti, la *pre-trial chamber* è chiamata a decidere se confermare le imputazioni formulate la *prosecutor* (V. FANCHIOTTI, *Struttura della Corte e fase delle indagini*, in Id. (a cura di), *La Corte penale internazionale. Profili sostanziali e processuali*, Torino, 2014, p. 131).

[78] M. MIRAGLIA, *Diritto di difesa e giustizia penale internazionale*, cit., p. 144.

ingiustificato[79], con significative ripercussioni su concreto esercizio del diritto al contraddittorio.

Ebbene, a fronte di indagini basate sempre più su dati *open access* ricavati dai *social media*, non sembra peregrino interrogarsi sull'effettività del "diritto alla *discovery* digitale", dal momento che la mole di informazioni raccolte potrebbe rendere *de facto* impossibile o, eccessivamente onerosa per la difesa, un'analisi completa delle stesse. Il problema non è certo nuovo, giacché può ben presentarsi (e, in effetti, si presenta) a livello nazionale con riguardo ai cd. maxiprocessi, cioè casi nei quali il compendio investigativo è costituito da un numero elevato di atti e documenti in formato analogico[80].

Nel caso di prove digitali costituite da materiale *open access* occorre necessariamente operare mediante l'impiego di *software* o algoritmi di IA che siano in grado di esplorare ed esaminare i contenuti pubblicati *online*; strumenti costosi, il cui utilizzo presuppone una conoscenza tecnica elevata. È in tale contesto, perciò, che rischia di manifestarsi una disparità tra accusa e difesa: le limitate risorse a disposizione dell'imputato non consentono di accedere alle migliori strumentazioni, residuando quale unica alternativa quella di affidarsi alle attività di verifica svolte dal pubblico ministero[81].

A tal proposito, peraltro, conviene rammentare che l'*equality of arms*, riconosciuta in numerose fonti sovranazionali[82] e considerata ormai un pilastro nell'ambito della procedura penale della ICC[83], non può che riverberare i suoi effetti anche nelle fasi antecedenti al processo. D'altro canto, non appare possibile ipotizzare una piena affermazione di questo principio nel contesto *strico sensu* processuale qualora «la stessa parità non sia stata perseguita e realizzata [anche] nella fase delle indagini»[84]. E, in effetti, la stessa giurisprudenza della ICC ha sviluppato il concetto di "parità delle armi" associandolo a quello di *fair trial*[85]: «*the ability of a party to a proceeding to adequately make its case, with a view to influencing the outcome of the proceedings in its favour*»[86].

---

[79] Trial Chamber, The Prosecutor v. Thomas Lubanga Dyilo, *Decision on the consequences of non-disclosure of exculpatory materials covered by Article 54(3)(e) agreements and the application to stay the prosecution of the accused, together with certain other issues raised at the Status Conference on 10 June 2008*, 15 giugno 2008.

[80] A tal riguardo, non sfugge come la dottrina più accorta abbia ipotizzato l'introduzione, a livello codicistico, di vere e proprie forme di "*discovery* 2.0". Per una recente trattazione, cfr. L. BARTOLI, *Parità delle armi e* e-discovery *nel processo penale: quali indicazioni da Strasburgo*, in R. Brighi (a cura di), *Nuove questioni di informatica forense*, Roma, 2022, p. 83 ss.

[81] Su tale rischio, v. M. DE ARCOS TEJERIZO, *Digital Evidence and fair trial rights at the International Criminal Court*, cit., p. 13 e 19, per il quale tutto ciò «*put the defense in a disadvantageous position from a very early stage of the proceedings*» (p. 13).

[82] *Ex plurimis*, artt. 10 e 11, Dichiarazione universale dei diritti umani, 1948; art. 14, Patto internazionale dei diritti civili e politici, 1966; art. 6, CEDU, 1950; art. 7, Carta dei diritti umani africana, 1981.

[83] In tal senso, v. M.C. BASSIOUNI, *Introduction to the International Criminal Law*, Londra, 2003, p. 612.

[84] Testualmente, M. MIRAGLIA, *Diritto di difesa e giustizia penale internazionale*, cit., p. 137, nt. 54.

[85] W.A. SCHABAS, *An Introducion to the Internatinal Criminal Court*, cit., p. 208 e, in part., nt. 88, ove si richiamano numerose pronunce in tal senso.

[86] Pre-Trial Chamber II, *The Prosecutor v. Joseph Kony and Vincent Otti, Decision on Prosecutor's Application for leave to appeal in part Pre-Trial Chamber II's Decision on the Prosecutor's applications for warrants of arrest under article 58*, 21 agosto 2005, par. 30.

In conclusione, e benché, nel contesto internazionale, il canone *de quo* non possa essere inteso quale parità delle risorse[87] (e, specialmente, delle risorse investigative[88]), non v'è dubbio che la *user-generated evidence* possa intaccare questo principio, con evidenti pregiudizi a carico dell'indagato. Come sottolineato da autorevole dottrina, sarebbe davvero contraddittorio un sistema – come quello della ICC – che si pone quale obiettivo principale la diffusione di una cultura dei diritti umani e la garanzia del loro rispetto, se, poi, in concreto, non riuscisse a garantire i diritti fondamentali degli accusati[89].

5. La fase giudiziale: ammissione e valutazione della prova

Il legame che intercorre tra i concetti di "presentazione", "ammissione" e "valutazione" delle prove nel contesto della ICC, come noto, è al centro di un acceso dibattito dottrinale[90]. Dal punto di vista normativo, l'art. 69, comma 4, St. ICC, attribuisce alla Corte la facoltà di pronunciarsi sull'ammissibilità del materiale raccolto nel corso delle *investigations* basando la propria decisione su tre distinti parametri (cd. *threepronged test*[91]): la prova è ammessa solo se rilevante per il caso di specie (*i*), tenendo conto del suo valore probatorio (*ii*) e di ogni pregiudizio che questa può arrecare allo svolgimento di un giusto processo (*iii*). In maniera speculare, l'art. 63, comma 2, delle *Rules of procedure and evidence* stabilisce che i giudici hanno la facoltà di valutare liberamente il compendio probatorio presentato dalle parti, al fine di determinarne la «*relevance or admissibility in accordance with article 69*» dello Statuto. In assenza di indicazioni chiare ed esplicite, la valutazione di ammissibilità probatoria – come riconosciuto dagli stessi giudici dell'Aia[92] – finisce per assumere un carattere ampiamente discrezionale, tanto da portare taluni autori ad affermare che la Corte, di fatto, «*admit whatever it likes*»[93].

Questa "flessibilità normativa" ha generato un contrasto interpretativo in merito all'individuazione della fase nella quale i giudici dovrebbero valutare l'ammissibilità del compendio probatorio, con evidenti ripercussioni sul concreto ed effettivo esercizio del diritto di difesa. Infatti, mentre l'art. 64, comma 1, *Rules of procedure and evidence* obbliga la parte a sollevare le questioni relative alla pertinenza e rilevanza nel momento in cui la

[87] In tal senso, Appeal Court, *Prosecutor v Kayishema and Ruzindana*, 1° giugno 2001, par. 72.

[88] Intese, queste ultime, come «*assets which improve the functioning capacity to search for, find and procure information and sources relating to the criminal charges against this defendant*», così C. JALLOH – A. DI BELLA, *Equality of Arms in International Criminal Law: Continuing Challenges*, in Y. Mcdermott – W.A. Schabas – N. Hayes (a cura di), *The Ashgate Research Companion to International Criminal Law-Critical Perspectives*, Londra, 2013, p. 263.

[89] M. DAMAŠKA, *What is the Point of International Criminal Justice?*, in *Chicago-Kent Law Review*, 2008, p. 355.

[90] Su tale aspetto, v., per tutti, H. FRIMAN, *Procedures of International Criminal Investigations and Prosecutions*, in E. Cryer – H. Friman – D. Robinson – E. Wilmshurst (a cura di), *An Introduction to International Criminal Law and Procedure*, Cambridge, 2010, p. 465 ss. Nella letteratura italiana, cfr. M. CAIANIELLO, *Amissione della prova e contraddittorio nelle giurisdizioni penali internazionali*, Torino, 2008, p. 113 ss.

[91] W.A. SCHABAS, *The International Criminal Court*, cit., p. 1087.

[92] Appeals Chamber, The Prosecutor v. Jean-Pierre Bemba Gombo, *Decision on the admission into evidence of materials contained in the prosecution's list of evidence*, 3 maggio 2011, par. 37.

[93] Per le due ultime citazioni, v. K. HIATT, *Open Source Evidence on Trial*, cit., p. 329.

prova è presentata in giudizio, la legge tace in merito al momento in cui la *Chamber* deve pronunciarsi su tale richiesta.

Sotto questo profilo, la struttura procedimentale appena descritta consente di distinguere tra un «*admission model*» e un «*production or submission model*»[94].

Stando a una prima corrente interpretativa[95], i giudici sono chiamati a prendere le proprie determinazioni in merito alla pertinenza, attendibilità, integrità e ammissibilità delle prove nel momento in cui queste sono presentate dalla parte, in modo da escludere tempestivamente dal fascicolo dibattimentale tutte ciò che appare irrilevante, consentendo così di avanzare nell'*iter* processuale «*on a clear and certain basis*»[96]. Una differente esegesi giurisprudenziale, invece, tende a rinviare la decisione sull'ammissibilità del compendio probatorio alla fase finale del procedimento, adottando un'unica pronuncia che ha ad oggetto tanto la pertinenza e la rilevanza della prova, quanto la sua credibilità e genuinità[97].

Nonostante l'art. 69 dello Statuto preveda che i giudici possano statuire *ex ante* sulla rilevanza della documentazione presentata dalle parti («*the Court may rule on the relevance or admissibility of any evidence*»), la maggioranza delle decisioni assunte dalla Corte penale internazionale sembrano propendere per un approccio del secondo tipo, obbligando *de facto* gli attori processuali a adottare un approccio cautelativo, dal momento che la strategia difensiva dovrà essere predisposta tenendo conto di tutto il compendio probatorio raccolto dal *prosecutor*.

Se l'adozione di un simile approccio appare generalmente criticabile, non v'è chi non veda come, *a fortiori*, esso sia destinato a ingenerare forti perplessità tutte le volte in cui il materiale investigativo sia costituto in prevalenza da fonti *open access*. A ben vedere, rinviare il giudizio di ammissibilità alla fase decisoria appare in contrasto con la natura *adversary* del modello adottato dalla Corte, antitetico rispetto a ragioni di economia ed efficienza processuale, nonché – e questo è il punto più significativo – lesivo del *right to defense*. In tal caso, infatti, la difesa, complice la voluminosità delle informazioni digitali, nonché l'estrema difficoltà nella loro analisi, è gravata da un onere processuale al quale non è in gradi di far fronte, vuoi per limiti temporali, vuoi economici.

Alla luce di tali considerazioni, pertanto, sarebbe auspicabile che la Corte accogliesse con risolutezza quell'approccio maggiormente garantista che impone di pronunciarsi tempestivamente sull'ammissibilità del materiale probatorio.

Nell'attesa di una sperabile modifica normativa (sulla quale, però, è lecito esprimere più di qualche perplessità), sembra comunque possibile proporre, *de lege lata*, un'interpretazione logico-sistematica che consente di addivenire alla soluzione qui proposta.

---

[94] Cfr. L. FREEMAN – R. VAZQUEZ LLORENTE, *Finding the Signal in the Noise*, cit., p. 181; F. GUARIGLIA, *"Admission" v. "Submission" of Evidence at the International Criminal Court*, in *Journal of International Criminal Court*, 2019, p. 315 ss.

[95] Cfr. Trial Chamber, The Prosecutor v. Thomas Lubanga Dyilo, *Decision on the admissibility of four documents*, 16 giugno 2008; Trial Chamber, The Prosecutor v. Germain Katanga, *Decision on the Prosecutor's Bar Table Motions*, 19 dicembre 2010.

[96] F. GUARIGLIA, *"Admission" v. "Submission" of Evidence at the International Criminal Court*, cit., p. 316.

[97] Cfr. Trial Chamber, The Prosecutor v. Laurent Gbagbo and Charles Blé Goudé, *Decision on the submission and admission of evidence*, 29 gennaio 2016; Trial Chamber, The Prosecutor v. Dominic Ongwen, *Initial Directions on the Conduct of the Proceedings*, 13 luglio 2016.

E si spiega.

Se l'art. art. 64, comma 1, *Rules of procedure and evidence*, come detto, obbliga la parte a sollevare le questioni relative alla pertinenza «*at the time when the evidence is submitted to a Chamber*», non si vede perché la stessa disposizione non possa essere interpretata nel senso di imporre alla Corte di pronunciarsi sull'ammissibilità nello stesso identico momento. D'altronde, parrebbe contraddittorio che la legge richieda alle parti di sollevare questioni relative alle prove in una determinata fase processuale, se i giudici possono comunque astenersi dal pronunciarsi in proposito, specialmente qualora «*the objection in question is to the effect that the evidence should not be received or considered as part of the trial*»[98]. Senza voler considerare, in aggiunta, come risulti tutt'altro che ragionevole un modello processuale nel quale il pubblico ministero può liberamente riversare nel processo una notevole quantità di prove documentali e audiovisive, senza fornire alcuna giustificazione sulla rilevanza di ogni singolo reperto[99]. Diversamente opinando, la difesa avrebbe l'onere di esaminare e contestare tutte le prove presentate dall'accusa, indipendentemente dalla loro rilevanza «e senza una chiara comprensione di come queste si colleghino alle accuse formulate dal *prosecutor*»[100].

[98] Così si esprime, nell'avallare tale impostazione, il giudice Eboe-Osuji nella *Concurring Separate Opinion* resa nel caso *Jean-Pierre Bemba Gombo* (Appeals Chamber, The Prosecutor v. Jean-Pierre Bemba Gombo, *Concurring Separate Opinion of Judge Eboe-Osuji*, 14 giugno 2018, parr. 301 ss.).

[99] In termini non dissimili si è espresso anche il giudice Henderson nella *Dissenting Opinion* resa nel caso *Laurent Gbagbo*, per il quale «*there is no point in cluttering the case record with exhibits whose relevance to the charges is not clearly demonstrated or that are of such doubtful probative value that no sensible Trial Chamber could reasonably base any findings upon them*» (Trial Chamber, *The Prosecutor v. Laurent Gbagbo and Charles Blé Goudé*, 1° giugno 2018, par. 12).

[100] Così, INTERNATIONAL BAR ASSOCIATION, *Recommendations of the International Bar Association ICC & ICL Programme to the Indipendent Expert Review of International Criminal Court*, 2020, p. 16 (trad. nostra).

CAPITOLO IV

FALSE FRIENDS TECHNIQUE E ACQUISIZIONE DI "DATI RISTRETTI"

SOMMARIO: 1. Artifizi e raggiri nelle piattaforme digitali: linee generali sull'impiego degli *undercover social network accounts* ad opera della polizia giudiziaria. – 2. Delimitazioni concettuali e caratteri fondamentali delle attività digitali sotto copertura. – 3. Criticità nell'inquadramento degli *undercover fake profiles*: verso una distinzione tra *monitor operation* e *interact operation*. – 4. La *false friends technique*: attività atipica di polizia giudiziaria. – 5. L'investigazione digitale sotto mentite spoglie: profili problematici della "richiesta di *follow*" tra *nemo tenetur se detegere* e libertà di autodeterminazione. – 6. Il concetto di "*privacy* interpersonale" quale limite all'impiego degli *undercover social network accounts*. – 7. Le "amicizie *online*" come fonte indiretta di informazioni: il caso del "*follower* cooperante". – 8. Investigazioni difensive e acquisizione di "dati ristretti". – 8.1 I limiti deontologici. – 8.2 I limiti normativi.

1. Artifizi e raggiri nelle piattaforme digitali: linee generali sull'impiego degli *undercover social network accounts* ad opera della polizia giudiziaria

Una differenza fondamentale tra i *social network* e le altre piattaforme della Rete – come, ad esempio, i *blog* o i siti *web* – è la possibilità per l'utente di limitare l'accesso a determinate informazioni presenti sul proprio profilo. È sempre più frequente, del resto, che i cibernauti impostino più stringenti *privacy settings*, in modo tale che le immagini, i video e ogni altra attività digitale compiuta in *Internet* siano visibile solo a una cerchia ristretta di soggetti individuati *ex ante*.

Dal punto di vista investigativo, tutto ciò induce a soffermare l'attenzione sull'*an* e sul *quomodo* dell'acquisizione di questi dati, cd. ristretti o «*quasi-private*»[1]. Nel contesto di uno Stato-ordinamento sempre più, per così dire, "astuto e sleale", il cui obiettivo è quello di «raccogliere con destrezza gli elementi che possono condurre alla pronuncia di condanna»[2], la moderna "polizia giudiziaria digitale" suole ricorrere con maggiore frequenza a una nuova metodologia di indagine, denominabile *false friends technique*, che si sostanzia nell'entrare "in contatto" con il *target* individuato mediante l'invio di una richiesta di "amicizia" o di una "richiesta di divenirne *follower*"[3]. In questo modo, l'autorità, utilizzando profili di copertura, riesce a visualizzare una serie di contenuti altrimenti inaccessibili, giacché l'utente ha scelto di renderli conoscibili solamente a una cerchia limitata di persone.

L'operazione in parola, a ben riflettere, sembra collocarsi a pieno titolo nel solco della tendenza recente, generalizzata e in costante sviluppo a ricercare e acquisire il contributo conoscitivo dell'indagato al di fuori delle sedi tradizionalmente a ciò deputate, cioè, in

[1] Su tale nomenclatura, cfr. Parte II, Cap. II, par. 2.

[2] L. LUPÁRIA, *La confessione dell'imputato nel sistema processuale penale*, Milano, 2006, p. 145.

[3] Cfr. R. LEVINSON-WALDMAN, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, in *Howard Law Journal*, 2018, p. 541-544, al quale si rinvia per l'analisi di alcuni casi pratici nei quali la polizia americana ha fatto ricorso a questa tecnica di indagine.

contesti formalmente procedimentalizzati all'interno del rito[4]. Ciò, però, non deve affatto stupire: lo sviluppo delle nuove tecnologie informatiche, difatti, ha offerto all'autorità inquirente una variegata gamma di artefatti in grado di apprendere e cristallizzare le dichiarazioni e i comportamenti tenuti dall'indagato *ante* ed *extra iudicium* (si pensi, ad esempio, all'impiego delle videoriprese investigative, dei droni o, ancora, delle registrazioni occulte captate dall'«agente segreto attrezzato per il suono»[5]).

Dal punto di vista *stricto sensu* giuridico, non v'è dubbio che il ricorso alla *false friends technique* abbia portata illecita, sia sotto il versante penalistico che quello civilistico.

Per un verso, la condotta dell'agente di polizia sotto mentite spoglie che crea un profilo *social* per fingere di essere altri integra il reato di sostituzione di persona (art. 494 c.p.), tanto nell'ipotesi in cui l'inquirente utilizzi un *nickname* o dati di contatto (nome, cognome, immagine di "copertina", etc.) riferibili a un altro soggetto[6], quanto nel caso in cui egli ricorra a identità di fantasia credibili e idonee a trarre in inganno i naviganti della Rete[7]. Del resto, la fattispecie incriminatrice, in un mondo nel quale le relazioni *online* vanno assumendo un'importanza crescente, integra un reato plurioffensivo, giacché non si limita a tutelare la fiducia della singola vittima tratta in inganno, ma anche la fiducia dell'intera comunità degli utenti. Questi ultimi, difatti, debbono poter fare «affidamento sulla lealtà delle identità con le quali intrattengono rapporti virtuali»[8]. Per altro verso, l'operazione viola i termini di servizio predisposti dai *social network providers*: la maggior parte dei gestori di piattaforme, invero, obbliga il cibernauta, al momento della registrazione (*rectius*, della stipula del contratto), a fornire informazioni personali veritiere[9].

Al netto di tali osservazioni, l'atto investigativo del quale si va discutendo può essere concretamente realizzato dalla polizia giudiziaria ricorrendo a due differenti modalità: a) creazione di un *fake profile* mediante l'utilizzo di un *nickname* di fantasia o di un *account*, pur contraffatto, ma riferibile a un soggetto che è effettivamente noto al bersaglio[10]; b) collaborazione da parte di un "amico virtuale" del *target* che, agendo su impulso dell'autorità investigativa, trasmette consapevolmente e volontariamente a quest'ultima dati e informazioni a lui accessibili[11].

---

[4] Ben più risalente nel tempo è, invece, la propensione di ogni sistema processuale penale a «vedere anche nell'imputato un "testimonio" in grado di fornire chiarimenti ed informazioni essenziali ed importanti in merito alla responsabilità penale personale» (così, A. GIARDA, *Persistendo 'l reo nella negativa*, Milano, 1980, p. 6).

[5] La felice espressione è di M. SCAPARONE, Common law *e processo penale*, Milano, 1974, p. 62.

[6] Cfr., tra le molte, Cass. pen., Sez. V, 22 giugno 2018, n. 42572; Cass. pen., Sez. V, 10 ottobre 2017, n. 4413.

[7] Cass. pen., Sez. II, 21 dicembre 2011, n. 4250.

[8] Testualmente, M. MARRAFFINO, *La sostituzione di persona mediante furto di identità digitale*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrati – A. Manna – M. Papa, Milano, 2023, p. 325.

[9] Si veda, ad esempio, quanto stabilito dal gestore di *Facebook*: *www.facebook.com/privacy/policy*.

[10] Quest'ultima ipotesi si rivela essere tanto efficace quanto problematica, giacché rappresenta una tecnica di inganno realizzabile esclusivamente in ambiente digitale (v. R. LEVINSON-WALDMAN, *Government Access to and Manipulation of Social Media*, cit., p. 548). Per più ampie considerazioni in merito all'impiego di operazioni investigative basate su artifici e raggiri e sulla loro maggiore intrusività rispetto a metodologie simili adoperate nel mondo analogico, v. W.A. LOGAN – J. LINFORD, *Contracting for Fourth Amendament Privacy Online*, in *Minnesota Law Review*, 2019, p. 101 ss. e, spec. p. 156.

[11] Cfr. *infra*.

In entrambe le ipotesi, ci si trova al cospetto di un'attività di indagine indubbiamente eccentrica rispetto alle tradizionali modalità di reperimento delle fonti di prova. Detta considerazione è destinata ad assumere una certa consistenza, dal momento che nella dottrina americana – che per prima si è interessata a questa tematica – si va prospettando, a tal proposito, un'analogia tra "mondo reale" e "mondo virtuale" destinata a generare più di qualche perplessità. Più in particolare, si afferma che un *restricted profile* sarebbe in tutto e per tutto equiparabile a una bacheca affissa in un edificio il cui accesso è subordinato al consenso del proprietario. Di conseguenza – si sostiene –, il cibernauta sarebbe portato a confidare sul fatto che quanto divulgato sul proprio "profilo chiuso" sia coperto da una certa aspettativa di riservatezza, perlomeno a fronte di un'intrusione *sine titulo* (cioè, in assenza di un *warrant*) da parte della polizia giudiziaria[12].

Il paragone, come si è anticipato, non appare pienamente convincente.

Nel contesto dei *social network*, infatti, gli "amici" ammessi alla "mensa virtuale" ben potrebbero diffondere e rendere pubbliche le informazioni a carattere riservato apprese in precedenza; informazioni che, in teoria, diverrebbero, a quel punto, liberamente accessibili a chiunque e, di conseguenza, anche alla polizia giudiziaria[13]. Grazie all'impiego della funzionalità *reposting*[14] o all'esecuzione di *screenshot*[15], ad esempio, soggetti estranei alla cerchia degli "amici" o dei *followers* non si limitano ad apprendere il contenuto dell'informazione, bensì la rappresentazione materiale della stessa (e, di riflesso, anche il suo contenuto). Da quest'angolo di visuale, perciò, è ragionevole affermare che l'utente, nel contesto delle nuove forme di comunicazione digitale, non possa vantare alcuna legittima pretesa di controllo assoluto sui propri dati aventi natura "ristretta"[16]. Nell'universo *social*, detto altrimenti, sembra perdere sempre più consistenza la distinzione – di matrice tedesca, ma importata in Italia sul finire degli anni Sessanta – tra i concetti di informazione «privata» (o «relativamente diffusa») e informazione «di pubblico dominio»[17], posto che l'interesse del mittente a limitare *ex ante* la conoscibilità di una certa informazione *online* appare, in questo contesto, una mera utopia.

---

[12] In questi termini, tra i primi, M.J. HODGE, *The Fourth Amendament and Privacy Issues on the New Interent: Facebook.com and Myspace.com*, in *Southern Illinois University of Law Journal*, 2006, p. 11.

[13] Concorde pure C.M. CORRELL, *Facebook, Crime Prevention, and the Scope of the Private Search Post-Carpenter*, in *Georgia Law Review*, 2022, p. 813.

[14] Con questa espressione si allude alla condivisione nel proprio *feed* di un contenuto riferibile a un altro utente.

[15] Trattasi dell'attività consistente nel "salvare", sotto forma di immagine, ciò che viene visualizzato sullo schermo del proprio dispositivo (fisso o mobile).

[16] Già nella "Risoluzione sulla tutela della *privacy* nei servizi di *social network*" adottata all'esito della trentesima Conferenza internazionale delle Autorità di protezione dei dati, tenutasi a Strasburgo il 15-17 ottobre 2008, le Autorità Garanti mettevano in guardia gli utenti dal «rischio di perdere il controllo dell'utilizzo dei propri dati una volta pubblicati in rete. Il fatto che si tratti di servizi operanti attraverso una "comunità" di utenti può far pensare che la situazione non sia molto diversa dal condividere informazioni con un gruppo di amici nel mondo reale; in realtà, le informazioni contenute nel proprio profilo possono raggiungere l'intera comunità degli abbonati al servizio – talora in numero di diversi milioni».

[17] Il riferimento è a F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen.*, 1967, p. 1085.

2. Delimitazioni concettuali e caratteri fondamentali delle attività digitali sotto copertura

Al fine di meglio delineare l'ambito della trattazione, occorre muovere da alcune precisazioni di natura concettuale.

Innanzitutto, è opportuno porre nuovamente l'accento sulla differenza che intercorre tra l'acquisizione con l'inganno di dati ristretti contenuti nei *social network* e l'attività *cyberpatrolling* esaminata nei capitoli precedenti. Il *discrimen*, come si è detto, va individuato nell'oggetto dell'attività "captativa": mentre il *social network monitoring* si sostanzia nella perlustrazione di fonti *open access*, nell'ipotesi *de qua agitur*, per contro, l'autorità inquirente è in grado di apprendere "dati ristretti", cioè visibili solamente a una cerchia limitata di persone[18].

Esclusa, dunque, ogni contiguità concettuale tra le due tecniche di indagine, l'attenzione dell'interprete parrebbe doversi orientare alle investigazioni digitali sotto copertura[19].

Com'è noto, però, l'*undercover agent* si presenta quale istituto poliedrico e di difficile inquadramento dogmatico. Onde rendersi conto di ciò, è sufficiente considerare come, in passato, la letteratura fosse propensa a identificare tale categoria solamente con la figura dell'agente provocatore, cioè quell'appartenente alla polizia giudiziaria che, dissimulando la propria identità, entrava in contatto con un bersaglio pre-individuato al fine di indurlo alla commissione di un reato. È solo sul finire degli anni Ottanta dello scorso secolo che la dottrina, nel solco di una lenta ma inesorabile «polverizzazione della nozione di agente provocatore»[20], prende consapevolezza dell'esistenza di attività sotto copertura diverse e ulteriori rispetto a quelle che mirano «ad incoraggiare la commissione di un reato ed a bloccare la condotta criminosa»[21].

Si giunge, così, alla elaborazione di una nuova categoria dogmatica focalizzata sulla figura dell'agente sotto copertura *lato sensu* inteso, un soggetto chiamato a realizzare investigazioni *undercover* assumendo una duplice, ma alternativa veste: agente infiltrato o agente provocatore[22]. Nel primo caso, l'autorità statale penetra nel tessuto criminale per acquisire notizie altrimenti inaccessibili; il poliziotto, in questa ipotesi, «si lascia provocare alla commissione di delitti, che poi spesso esegue lui stesso, sia per non rivelare la sua

---

[18] In questo senso, v. quanto affermato nel *report* redatto dal CONGRESSIONAL RESEARCH SERVICE, *Law Enforcment and Techonology: Using Social Media*, 11 gennaio 2022, p. 4, ove si sottolinea come in tali circostanze «*law enforcement does not have public access to information*». Concordi, in dottrina, C. CONTI – M. TORRE, *Spionaggio digitale nell'ambito dei* social network, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 553. *Contra*, A. APRUZZESE, *La recente normativa in tema di contrasto del terrorismo e del proselitismo tramite* web. *Nuovi modelli di normative di prevenzione e nuovi schemi di indagini proattive*, in AA.VV., *La giustizia penale preventiva. Ricordando Giovanni Conso*, Milano, 2016, p. 234, che equipara l'accesso alle informazioni pubblicamente disponibili sui *social* all'accesso ai dati riservati «agli "amici" degli utenti».

[19] Per un'ampia trattazione del tema, v., di recente, P. TROISI, *Le investigazioni digitali sotto copertura*, Bari, 2022.

[20] C. DE MAGLIE, *L'agente provocatore. Un'indagine dommatica e politico-criminale*, Milano, 1991, p. 242, la quale definisce questo passaggio come «un'autentica novità nello sviluppo dottrinale [italiano]».

[21] Così, nell'illustrare i caratteri dell'agente provocatore, V. FANCHIOTTI, voce *Agente sotto copertura*, in *Enc. dir.*, Annali VIII, Milano, 2015, p. 10.

[22] Secondo C. DE MAGLIE, *L'agente provocatore*, cit., p. 243, si tratta di due figure non solo «strutturalmente» diverse, «ma addirittura antictich[e]».

identità, sia per penetrare più a fondo nella struttura dell'organizzazione»[23]. Nella seconda ipotesi, invece, l'inquirente sotto mentite spoglie istiga o agevola causalmente la commissione di un illecito penale.

Anche la Corte di Strasburgo, del resto, ha avuto modo di pronunciarsi a più riprese in merito al concetto di "operazione sotto copertura". Fin dal *leading case Texeira de Castro c. Portogallo*[24], i giudici europei hanno riposto particolare attenzione alla distinzione tra *undercover agent* e *agent provocateur*. Quanto al primo, l'attività realizzata dalle forze dell'ordine va considerata legittima, giacché limitata alla mera presa di contatto con il bersaglio, al fine di osservare e raccogliere informazioni sull'andamento dell'*iter criminis*[25]. Circa il secondo, invece, l'operazione è destinata a porre non pochi problemi di compatibilità con il *fairness* processuale e l'equità del giudizio (art. 6, par. 1, CEDU), posto che l'agente realizza una vera e propria "determinazione al reato".

Al di là di ciò, v'è chi ha notato come, nella prassi, la distinzione si mostra assai più sfumata, tanto che l'attività dell'agente sotto copertura appare in perenne contiguità con la provocazione o l'istigazione. Infatti, si è efficacemente osservato come «chi agisce per "scoprire" qualcosa, per ottenere informazioni investigative, sia pur inconsciamente, si mette nella prospettiva ed orienta il discorso ad addurre provocatoriamente l'*argumentum*»[26]. La difficoltà nel discernere tali categorie emerge in maniera ancora più evidente dalla semplice lettura di alcune, recenti prese di posizione della giurisprudenza di legittimità, nelle quali il Supremo consesso si riferisce «all'agente infiltrato» come a colui che ha «determinato l'indagato alla commissione di un reato»[27].

Al netto della condivisibilità o meno di tali classificazioni, entrambe le attività, come si è detto, debbono essere ricomprese nell'alveo di un'unica macrocategoria: le "operazioni sotto copertura"[28]. In ambedue i casi, infatti, l'agente statale dissimula la propria vera identità con l'obiettivo di entrare in contatto e interagire con uno specifico bersaglio. Il rapporto dialogico tra l'agente *undercover* e il *target* di riferimento diviene, perciò, l'elemento specializzante la fattispecie[29], tanto che la condotta dell'operatore sotto copertura risulta perlopiù calibrata a seconda del comportamento tenuto dall'obiettivo.

Quanto appena sostenuto sembra confermato dal dettato letterale di quello che viene ormai comunemente definito lo "statuto generale" delle attività *undercover*. Ai sensi dell'art. 9, comma 2, l. 146/2006[30], gli ufficiali e gli agenti di polizia giudiziaria possono utilizzare

---

[23] Così, ancora, C. DE MAGLIE, *L'agente provocatore*, cit., p. 243.

[24] Corte edu, 9 giugno 1998, *Texeira de Castro c. Portogallo*.

[25] Corte edu, 21 marzo 2002, *Calabrò c. Italia e Germania*.

[26] F.R. DINACCI, *L'agente sotto copertura e reati contro la pubblica amministrazione: nuovi difetti e vecchi vizi*, in *Arch. pen.* web, 4 maggio 2020, p. 13.

[27] Cass. pen., Sez. II, 19 gennaio 2022, n. 8580. Ad ogni modo, è opportuno segnalare come la giurisprudenza abbia riconosciuto l'inutilizzabilità della prova acquisita in caso di operazioni sotto copertura consistenti nell'incitamento o nell'induzione alla commissione di un reato (cfr., *ex multis*, Cass. pen., Sez. VI, 4 febbraio 2020, n. 12204; Cass. pen., Sez. VI, 11 dicembre 2014, n. 51678).

[28] Per questa opinione, v. anche G. BAROCCU, *Le indagini sotto copertura*, Napoli, 2011, p. 29.

[29] Su tale carattere del metodo investigativo *undercover*, v., esplicitamente, N. VENTURA, *Le investigazioni* under cover *della polizia giudiziaria*, Bari, 2008, p. 15.

[30] L. 16 marzo 2006, n. 146, con la quale l'ordinamento italiano ha ratificato e dato esecuzione alla Convenzione e ai Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 e il 31 maggio 2001.

documenti, identità o indicazioni di copertura «per attivare o entrare in contatto con soggetti e siti nelle reti di comunicazione». Allo stesso modo, l'art. 14, comma 2, l. 269/1998, prevede che il personale di polizia postale possa «utilizzare indicazioni di copertura» anche per «attivare siti nelle reti, realizzare o gestire aree di comunicazione o scambio su reti o sistemi telematici, ovvero per partecipare ad esse». Tutt'e due le definizioni normative sembrano identificare nell'instaurazione di un vero e proprio "dialogo relazionale" («entrare in contatto», «partecipare», etc.) il requisito sufficiente e necessario per la riconducibilità di un'operazione investigativa nel novero delle attività *undercover* in senso stretto.

3. Criticità nell'inquadramento degli *undercover fake profiles*: verso una distinzione tra *monitor operation* e *interact operation*

Alla luce di tale inquadramento teorico, è possibile esaminare più da vicino l'attività di *undercover Internet investigation* oggetto di studio.

Innanzitutto, occorre distinguere due ipotesi che, apparentemente legate da caratteristiche comuni, debbono essere tenute concettualmente distinte. In particolare, l'autorità investigativa, dopo aver acquisito con l'inganno l'accesso alle informazioni ristrette contenute nel profilo *social* del bersaglio, potrebbe astrattamente realizzare una duplice operazione: a) acquisizione *una tantum* di un dato o monitoraggio continuativo e occulto del profilo[31]; b) interazione diretta con il *target*, al fine di acquisire dichiarazioni o indurlo alla commissione di un reato. La necessità di differenziare dette attività è ben evidenziata nelle *guidlines* redatte dall'*American Department of Justice, Criminal Division, Computer Crime and Intellectual Property*, con le quali l'autorevole autorità d'oltreoceano ha messo in luce le innumerevoli potenzialità legate all'impiego dei *social network* nella fase delle *investigations*[32]. Nel *report*, più in particolare, si sottolinea come le operazioni *undercover* svolte nelle piattaforme digitali consentano di realizzare, distintamente, tanto una «*communicate with suspects/targets*», ovverosia un'interazione diretta e immediata con il bersaglio, quanto un semplice «*gain access to non-public information*»[33].

Preso atto, dunque, della necessità di distinguere tra una *monitor operation* e una *interact operation*[34], non pare revocabile in dubbio che quest'ultima attività debba essere annoverata a pieno titolo nell'orbita delle operazioni digitali sotto copertura. In tale evenienza, infatti, la polizia giudiziaria, dopo aver acquisito con l'inganno l'"amicizia" del soggetto preso di mira, riesce a instaurare con quest'ultimo un vero e proprio "dialogo interattivo", attraverso lo scambio di messaggi in canali chiusi di comunicazione. Dette operazioni, dunque, debbono ritenersi legittime, nell'ordinamento italiano, solamente se svolte con riguardo a quelle fattispecie criminose per le quali la legge consente il ricorso all'agente sotto copertura.

---

[31] Sulla distinzione tra *una tantum surveillance* e monitoraggio continuativo, cfr. Parte II, Cap. II.

[32] DEPARTMENT OF JUSTICE, CRIMINAL DIVISION, COMPUTER CRIME AND INTELLECTUAL PROPERTY, *Obtaining and Using Evidence from Social Networking Sites*, 3 marzo 2010, p. 32.

[33] *https://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf*.

[34] Sulla necessità di una tale distinzione, v. anche R. LEVINSON-WALDMAN, *Private Eyes, Thery're Watching You: Law Enforcement's Monitoring of Social Media*, in *Oklahoma Law Review*, 2019, p. 999; T.A. HOFFMEISTER, *Social Media in the Courtroom. A New Era for Criminal Justice?*, Santa Barbara, 2014, p. 67 s.

Non risulta altrettanto agevole, per contro, ricondurre alla medesima categoria quelle operazioni di indagine con le quali l'autorità inquirente si limita a utilizzare un *undercover social media account* per ottenere l'"amicizia" del bersaglio, senza intrattenere alcun rapporto diretto con quest'ultimo, e con il solo obiettivo di raccogliere e conservare dati digitali (*una tantum* o in maniera sistematica). Come si è visto, infatti, la normativa in tema di agente *undercover* identifica nel "contatto relazionale e dialogico" fra l'autorità inquirente e il bersaglio il requisito necessario per ricondurre un'operazione investigativa a tale *genus*.

A fronte di ciò, la *quaestio iuris*, per quel che interessa in questa sede, si sostanzia nel chiedersi se il mero invio di una richiesta di "amicizia virtuale" possa essere ricompreso nella nozione di "interazione", così per come enucleata nel contesto delle attività coperte.

La risposta al quesito parrebbe negativa.

In effetti, non sembra che la semplice "richiesta di contatto" possa assurgere, di per sé sola, a elemento qualificante un'attività *undercover*, pur se eseguita in ambiente digitale[35]. È ben vero – si dirà – che in questo caso ci troviamo di fronte a un travisamento dei ruoli, elemento specializzante l'attività sotto copertura. Ed è altrettanto vero che il semplice invio di una richiesta di "connessione *social*" potrebbe essere letto come un atto prodromico rispetto a un'operazione undercover intesa in senso stretto. Ciò nondimeno, come detto, il «contatto» al quale si allude generalmente nel contesto delle investigazioni coperte implica l'instaurarsi di una "relazione interpersonale" fra l'agente in borghese e il *target*, volta all'apprensione di informazioni processualmente rilevanti; tant'è che, nella prassi, la condotta del primo è strutturalmente calibrata sul comportamento tenuto dall'obiettivo. Del resto, la stessa Corte di cassazione ha espressamente escluso dal novero delle "operazioni di contrasto sotto copertura" quelle ipotesi in cui non sia ravvisabile alcuna particolare «attività stimolatrice o provocatoria» che si sostanzia «nella strumentale intrusione nel mondo dell'illecito al fine di agevolare la scoperta dei suoi protagonisti»[36].

4. La *false friends technique*: attività atipica di polizia giudiziaria

Esclusa ogni riconducibilità al contesto delle *digital undercover investigations*, le operazioni di *police fishing* (si legga, *monitor operation*) potrebbero essere annoverate nella categoria delle attività atipiche di polizia giudiziaria, per lo svolgimento delle quali la legge non richiede alcun *placet* autorizzativo (artt. 55, 348 e 370 c.p.p.). La dottrina (italiana e straniera), del resto, ha sostenuto che in dette ipotesi l'utente accetta liberamente e senza costrizioni di entrare in contatto con il "falso poliziotto", cosicché nessuna aspettativa di

[35] Concorde A. GILLESPIE, *Regulation of Internet Surveillance*, in *European Human Rights Law Review*, 2009, p. 564. *Contra*, invece, P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 91, 181. Pure M. MARRAFFINO, *La sostituzione di persona mediante furto di identità digitale*, cit., p. 326, sembra ricondurre la semplice operazione «di chi chieda l'amicizia su *Facebook* a un soggetto» nell'ambito delle attività sotto copertura, essendo irrilevante che l'agente «poi eventualmente lo inviti a chattare su determinati argomenti». In quest'ultimo senso si esprime anche M. TORRE, Open source intelligence: *spionaggio digitale e* social network, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 1718, il quale, però, al pari degli altri A. sopra richiamati, non distingue tra *monitor operation* e *interact operation*.

[36] Cass. pen., Sez. V, 19 gennaio 2004, n. 21778.

privacy potrebbe essere legittimamente invocata[37]. Se il dichiarante ha errato nella scelta del suo interlocutore – si è affermato –, non potrà che dare la colpa "solo a sé stesso". La volontarietà del consenso manifestato dal prevenuto, in questa prospettiva, assume una sorta di efficacia sanante rispetto all'intrusione nella sfera di riservatezza dell'individuo. Ne consegue, sul piano investigativo, la legittimità dell'operazione "captativa" e, sul versante *stricto sensu* probatorio, la piena utilizzabilità del materiale acquisito.

L'interpretazione avanzata si spinge fino a operare una vera e propria equiparazione, dal punto di vista processuale, tra le *public available information* e le *quasi-private infomation*[38]. Anche queste ultime, infatti, dovrebbero essere considerate "liberamente e pubblicamente disponibili", giacché qualora gli utenti condividano le proprie *communications* o i propri dati a un numero limitato di "amici" o *followers*, questi potrebbero scegliere, a loro volta, di divulgarli a un numero indeterminato di persone. Da questo punto di vista, perciò, nessuno potrebbe vantare una legittima aspettativa di *privacy* nei *social network* a causa dell'intrinseca interconnettività di questi strumenti di comunicazione[39].

In detta cornice teorica, è interessante osservare come l'esegesi proposta sembra essere indirettamente avallata pure da un'analisi sistematica della giurisprudenza d'oltreoceano[40]. Nel caso *Gatson c. Stati Uniti*[41], ad esempio, la polizia giudiziaria, pur in assenza di un *warrant* emesso dal giudice, aveva inviato una richiesta di *follow* al profilo *Instagram* in uso all'imputato, al fine di accedere alle informazioni che quest'ultimo aveva scelto di mantenere ristrette. Ad avviso dei giudici, i dati ottenuti dovevano ritenersi legittimamente utilizzabili in applicazione della *Third party doctrine*, in base alla quale ogniqualvolta un individuo trasferisce senza alcuna costrizione a terzi (*person or entity*) un certo bagaglio conoscitivo (pubblico, privato o riservato), egli perde ogni aspettativa di riservatezza e, consequenzialmente, si assume il rischio che il destinatario possa essere anche un agente di polizia sotto mentite spoglie.

In detti casi, la giurisprudenza nordamericana, dunque, fatica a rinvenire una qualche frizione con il diritto alla riservatezza e al rispetto della vita privata.

In primo luogo, l'esclusione di una legittima aspettativa di *privacy* in senso soggettivo sarebbe giustificata dal fatto che l'indagato ha accettato volontariamente la richiesta di "amicizia" pervenuta dall'agente *undercover*, scegliendo deliberatamente di rendere conoscibili informazioni ristrette a un perfetto sconosciuto. L'assunto si giustifica alla luce

[37] Per tale opinione, v., ad es., S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 83. Nello stesso senso, v. A. GILLESPIE, *Regulation of Internet Surveillance*, cit., p. 564; C. CONTI – M. TORRE, *Spionaggio digitale nell'ambito dei* social network, cit., p. 560; B. MUND, *Social Media Searches ad the Resonable Expectation of Privacy*, in *Yale Journal of Law & Technology*, 2017, p. 253, per il quale «*the mere request to join a private social network does not violate any privacy interest*».

[38] Su tale classificazione, cfr., Parte II, Cap. II, par. 1.

[39] In questi termini, v. E. NORTH, *Facebook Isn't Your Space Anymore: Discovery af Social Networking Websites*, in *Kansas Law Review*, 2010, p. 1296 s.; E.W. SHOLL, *Exhibit Facebook: The Discovery and Admissibility of Social Media Evidence*, in *Tulane Journal of Technology and Intellectual Property*, 2013, p. 212.

[40] Cfr., *amplius*, M. JACKSON JONES, *Shady Trick or Legitimate Tactic – Can Law Enforcement Officials Use Fictitious Social Media Accounts to Interact with Suspects*, in *American Journal of Trial Advocacy*, 2016, p. 69 ss.

[41] *Gatson c. Stati Uniti*, 3d 312, 325 (5th Cir. 2014). Conformi, *Stati Uniti c. Robison* Case No. 11CR380 (DWF/TNL); *Stati Uniti c. Stratton*, 229 F. Suppl. 3d 1230, 1241 (D. Kan. 2017).

della cd. *misplaces confidences doctrine* o *misplace trust doctrine*, una variante della "dottrina della terza parte" che trae le proprie origini dalla nota pronuncia *Hoffa c. Stati Uniti*[42]. In quella sede, la Corte americana ha affermato che le informazioni divulgate spontaneamente a un informatore sotto copertura non sono coperte da una legittima aspettativa di *privacy* e, dunque, non soggiacciono alla protezione offerta dal IV emendamento. D'altro canto, una fiducia mal riposta (*misplaced confidence*) nell'interlocutore è un fatto in tutto e per tutto addebitabile all'utente[43]. A conclusioni non dissimili, peraltro, dovrebbe giungersi anche qualora la polizia giudiziaria ricorra all'utilizzo di un profilo *fake* riferibile a una persona già nota all'indagato, giacché, pure in questa ipotesi, il soggetto presta il consenso alla diffusione delle proprie informazioni.

In secondo luogo, non sarebbe neppure ravvisabile una violazione della *expectation of privacy* nella dimensione oggettiva, poiché, fin dalla nota sentenza *Katz c. Stati Uniti*, la collettività non è disposta a riconoscere come ragionevole l'aspettativa di *privacy* di un soggetto che ha scelto di divulgare «pubblicamente» informazioni private (e, dunque, a maggior ragione, "ristrette")[44]. Al compimento dell'atto di condivisione, infatti, egli si assume consapevolmente il rischio che uno dei propri *followers* possa inoltrarle a terzi. È questa, del resto, un'alea insita in qualunque relazione umana, sia digitale sia reale[45].

Sennonché, le argomentazioni richiamate a sostegno dell'irrilevanza del metodo fraudolento ai fini dell'acquisizione probatoria (*rectius*, ai fini dell'applicabilità del IV emendamento) hanno generato più di qualche perplessità, tanto da indurre una parte della giurisprudenza a discostarsi, in maniera più che convincente, dall'orientamento maggioritario[46].

Innanzitutto, occorre considerare che l'aspettativa di riservatezza di un fruitore dipende, tra l'altro, dalle impostazioni di *privacy* adottate. Si vuol dire, cioè, che, qualora il *social network* venisse utilizzato in maniera da escludere il pubblico dalla visione di determinati contenuti, ciò dimostrerebbe la volontà del cibernauta di mantenere una certa ristrettezza dei dati[47].

Inoltre, il riferimento alla *Third party doctrine* parrebbe all'evidenza inconferente. Nel caso che ci occupa, le informazioni condivise dall'utente non possono essere qualificate come *public available* (requisito indispensabile per l'operatività della dottrina *Katz*): trattasi, come detto, di dati ristretti. A tal proposito, peraltro, a nulla varrebbe obiettare che il destinatario finale di tali contenuti (si legga, l'"amico virtuale") potrebbe comunque

[42] *Hoffa c. Stati Uniti*, 385 U.S. 293 (1966).

[43] Sostiene questa esegesi N. PETRASHEK, *The Fourth Amendament and the Brave New World of Online Social Networking*, in *Marquette Law Review*, 2010, p. 1525.

[44] *Katz v. United States*, 389 U.S. 347 (1967): «*what a person knowingly exposes to the public [...] is not a subject of Fourth Amendment protection*».

[45] M. BEDI, *Social Network, Government Surveillance, and the Fourth Amendament Mosaic Theory*, in *Boston University Law Review*, 2014, p. 1873-1875.

[46] Cfr., ad es., *Stati Uniti c. Chavez*, 423 F. Supp. 3d 194 (2019).

[47] *Stati Uniti v. Westley*, No. 3:17-CR-171, 2018 WL 3448161 (D. Conn. 17 luglio 2018). In proposito, v. le puntuali osservazioni di S. SIGNORATO, *Le indagini digitali*, cit., p. 64 s., secondo cui qualora la piattaforma venisse impiegata «con una sorta di aspettativa di riservatezza rafforzata», come nel caso in cui «il numero delle persone con cui vengono condivise le informazioni sia selettivo», tale spazio si potrebbe configurare come «una forma di estensione "abitativa", inquadrabile come domicilio».

divulgarli alle forze dell'ordine. Occorre tenere ben distinti, infatti, il rischio, gravante sul mittente, che il destinatario delle informazioni possa ri-condividerle – anche con l'autorità investigativa – e, per contro, quello che la polizia giudiziaria possa utilizzare artifizi e raggiri per acquisirle. È senz'altro vero che il IV emendamento non protegge l'errata convinzione che la persona alla quale un soggetto ha volontariamente confidato i suoi segreti non li rivelerà a terzi. Ciò nonostante, l'autorità inquirente, nell'ipotesi in esame, ottiene le informazioni direttamente dal bersaglio-indagato, senza che vi sia alcun contatto con un intermediario-collaboratore.

Infine, desta qualche perplessità anche l'idea che l'imputato non possa vantare una legittima aspettativa di *privacy* nei confronti di qualsiasi contenuto pubblicato sui *social media*, dal momento che egli avrebbe volontariamente trasmesso tali informazioni all'*Internet service provider*. Il gestore della piattaforma, infatti, non può essere considerato come un "terzo" rispetto al quale qualsiasi comunicazione perde ogni aspettativa di riservatezza. Questi, più correttamente, si limita a mettere a disposizione uno "spazio" nel quale gli utenti possono intrattenere le proprie relazioni. Trattasi, dunque, di un mero intermediario che non svolge alcuna funzione nel rapporto sociale instauratosi tra le parti. Del resto, è proprio la giurisprudenza americana più recente ad aver sottolineato come la *Third party doctrine* non possa trovare applicazione con riguardo a tutte quelle informazioni «non dirette a un'azienda, ma semplicemente inviate tramite l'azienda»[48]. Per tale ragione, i *post* e i messaggi ristretti presenti sui *social network* non possono certamente qualificarsi come "diretti" all'*Internet service provider*; quest'ultimo, piuttosto, si limita ad assumere il ruolo di «intermediatore» attraverso il quale dette informazioni sono divulgate ai destinatari finali[49].

5. L'investigazione digitale sotto mentite spoglie: profili problematici della "richiesta di *follow*" tra *nemo tenetur se detegere* e libertà di autodeterminazione

Facendo leva sulle predette argomentazioni, alcuni Autori, seppur con differenti accenti, hanno sottolineato come qualora l'attività *undercover* sia subordinata a un'accettazione o, comunque, a un consenso del bersaglio e risulti finalizzata al «semplice approvvigionamento di dati, senza avviare dialoghi con l'utente, a monte si staglia [comunque] il travisamento di ruoli e funzioni, elemento qualificante delle attività coperte»[50]. Di conseguenza, l'utilizzo di artifizi e raggiri onde essere ammessi in luoghi altrimenti inaccessibili renderebbe viziato il consenso ottenuto con l'inganno. La dottrina statunitense, a questo proposito, ha coniato, da tempo, l'efficace espressione «*ignorant consent*»[51] proprio per descrivere una manifestazione di volontà carpita dalla polizia giudiziaria ricorrendo a sotterfugi, inganni e artifici che contemplano l'impiego di identità fittizie per acquisire informazioni ristrette.

[48] *Johnson c. Duxbury*, 931 F.3d 102, 108 1st Cir. 2019 (trad. nostra).

[49] *Stati Uniti c. Chavez*, cit. (trad. nostra). Ma, in forma dubitativa rispetto a questa conclusione, v. M.J. HODGE, *The Fourth Amendament*, cit, p. 113.

[50] P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 181.

[51] M. CLOUD, *Ignorance and Democracy*, in *Texas Tech Law Review*, 2007, p. 1168.

Il richiamo alla condotta fraudolenta realizzata dall'agente di polizia quale snodo esegetico per sostenere l'inutilizzabilità delle informazioni raccolte[52] rievoca il dibattito sviluppatosi – e tutt'ora in essere – con riguardo all'impiego del *trojan horse* nel corso della fase investigativa. Anche in quel contesto, a ben vedere, è possibile rinvenire un'attività intrusiva della polizia giudiziaria che, mediante un'azione fraudolenta, sfrutta la collaborazione del bersaglio per acquisire informazioni altrimenti inaccessibili. È noto, infatti, che, nella prassi, l'autorità inquirente, qualora non possa inoculare direttamente il *virus* nel dispositivo mobile in uso all'utente, ricorra a stratagemmi sempre più sofisticati e invasivi per indurre quest'ultimo a un'auto installazione del *virus*. Si pensi, ad esempio, all'invio di una *e-mail* al *device* da monitorare, all'inoltro di aggiornamenti in realtà non necessari e al blocco delle chiamate in uscita[53].

Il richiamato parallelismo tra la *false friends technique* e l'impiego del cavallo di troia induce a soffermarsi sulla delicata tematica concernente la possibilità di considerare la collaborazione attiva del *target*-indagato (ovverosia, l'accettazione della richiesta di "amicizia") alla stregua di un atto lesivo del *nemo tenetur se deterege*.

Non è certo questa la sede per soffermarsi, *funditus*, sulle numerose, variegate e, alle volte, contraddittorie definizioni offerte in relazione a un concetto che pecca di una singolare vaghezza tanto nei contenuti, quanto nell'ambito applicativo. A conferma della costante «instabilità concettuale»[54], è sufficiente osservare come «tale principio, nelle molteplici varianti della sua formulazione latina, sia stato spesso richiamato con riguardo ad una gamma di comportamenti piuttosto eterogeni»[55]. Esso, come noto, costituisce l'espressione di tre differenti prerogative: il diritto a non essere interrogato (*right not to be questioned*), il diritto a non autoincriminarsi (*privilege against self-incrimination*) e il diritto al silenzio in senso stretto (*right to be in silence*)[56]. Il *nemo tenetur edere contra se*, in questa prospettiva, è stato talvolta riferito alle sole «dichiarazioni» verbali o scritte (autoaccusatorie[57] o *lato*

[52] P. TROISI, *Le investigazioni digitali sotto copertura*, cit., p. 134, il quale critica aspramente l'idea di «porre il *focus* sul contegno del bersaglio (che ha volontariamente condiviso la notizia, si è accollato il rischio che sia diffusa, ha errato nella scelta dell'interlocutore), anziché sull'inganno orchestrato dalla pubblica autorità».

[53] Le analogie, però, si arrestano qui. L'impego della "cimice di Stato" in modalità intercettazione (e non solo), invero, consente all'autorità procedente di acquisire tendenzialmente dati segreti e riservati, cioè che l'indagato ha scelto di non condividere con terzi. Al contrario, come si è detto, il ricorso a profili *fake* da parte delle forze dell'ordine è volto esclusivamente all'apprensione di informazioni ristrette.

[54] M.S. GREEN, *The Privilege's Last Stand: the Privilege Against Self-Incrimination and the Right to Rebel Against the State*, in *Brooklyn Law Review*, 1999, p. 628.

[55] V. GREVI, *Nemo tenetur se detegere: interrogatorio dell'imputato e diritto al silenzio nel processo penale italiano*, Milano, 1972, p. 3 s.

[56] Su tale classificazione, v., per tutti, E. AMODIO, *Diritto al silenzio o dovere di collaborazione? A proposito dell'interrogatorio dell'imputato in un libro recente, in Riv. dir. proc.*, 1973, p. 412.

[57] Nel senso di un diritto a non "dichiarare la propria colpevolezza", v. M. SCAPARONE, *Commento all'art. 24, secondo comma, Cost.*, in G. Branca (a cura di), *Commentario della Costituzione. Rapporti civili (artt. 24-26)*, Bologna, 1981, p. 91, secondo cui il *nemo tenetur se detegere* «concerne i profili tanto del diritto al silenzio […] quanto del diritto a non autoincriminarsi […] inteso come diritto a non rendere dichiarazioni da cui potrebbe emergere una propria responsabilità per fatti diversi da quello per cui si procede, nonché più in generale, come comprensivo pure del diritto a non effettuare dichiarazioni confessorie sui fatti di cui si è accusati)».

sensu intese[58]?) rese dall'indagato/imputato nel corso del procedimento (tanto in sede istruttoria, quanto in sede dibattimentale); talaltra, alle «condotte collaborative» tenute con l'autorità inquirente (autoincriminanti[59] o in senso lato[60]?); o, ancora, a un vero e proprio diritto di non collaborare con l'accusa e, dunque, di non contribuire in alcun modo alla dimostrazione della propria colpevolezza[61].

Al netto delle differenti fisionomie assunte dal canone *de quo*, un dato sembra emergere con nettezza: il diritto a non autoincriminarsi è destinato a trovare applicazione solo qualora vi sia un contatto diretto e immediato (nel senso di non-mediato) tra l'imputato e l'autorità procedente. La *ratio essendi* del principio, del resto, va identificata nella necessità di impedire che l'indagato sia indotto, tramite coartazione fisica o psicologica – da parte degli organi del procedimento penale – a rendere dichiarazioni *contra se* o, a seconda della lettura che si intenda prediligere, ad "agire a proprio danno[62].

L'assunto affonda le proprie radici nella celebre opera con la quale autorevole dottrina[63] ebbe modo di affermare che la garanzia del diritto al silenzio non può trovare applicazione alcuna con riferimento alle dichiarazioni autoaccusatorie captate nel corso di un'intercettazione telefonica. In tali casi, non vi è alcun pericolo, neppure in astratto, che l'indagato possa essere influenzato o indotto a modificare la propria volontà dichiarativa. Durante l'intercettazione, infatti, il bersaglio è ignaro di essere occultamente ascoltato, e proprio questa caratteristica del mezzo di ricerca della prova, per quanto «"odiosa", ed in un certo senso immorale […] consente di distinguere l'ipotesi *de qua* dalle ipotesi cui si riferisce

---

[58] Per un'interpretazione del canone *de quo* come diritto dell'accusato a non fornire prove di "natura dichiarativa", v. E. AMODIO, *L'esame dell'imputato e la sua mutazione genetica*, in *Discrimen*, 5 luglio 2023, p. 4.

[59] S. SIGNORATO, *Le indagini digitali*, cit., p. 238. Cfr., altresì, il Considerando n. 25 della direttiva 2016/343/UE, ove si stabilisce che «gli indagati e imputati, se invitati a rilasciare dichiarazioni o a rispondere a domande, non dovrebbero essere costretti a produrre prove o documenti o a fornire informazioni che possano condurre all'autoincriminazione». Anche la COMMISSIONE DELLE COMUNITÀ EUROPEE, *Libro verde sulla presunzione di non colpevolezza*, Bruxelles, 2006, COM (2006-174 def.), par. 2.4, si riferisce a un diritto «a non essere obbligato a fornire prove di colpevolezza».

[60] V. MANZINI, *Trattato di diritto penale italiano*, vol. V, in G.D. Pisapia (a cura di), *Delitti contro l'amministrazione della giustizia*, Torino, 1982, p. 543, per il quale «la libertà dalle autoincriminazioni [garantita all'art. 24, comma 2, Cost.] comprende […] il diritto di non essere costretto a porre in essere alcun comportamento, anche non consistente in dichiarazioni, il quale possa pregiudicare il suo autore nello svolgimento di una difesa nel processo».

[61] Per questa visione estensiva, v. L. LUPÁRIA, Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, diretto da G. Spangher, in G. Garuti (a cura di), *Modelli differenziati di accertamento*, t. I, Torino, 2011, p. 388, per il quale l'indagato non è «mai sottoponibile a un dovere di concorrere alla propria incriminazione tramite comportamenti collaborativi (*nemo tenetur se detegere*)»; O. MAZZA, *Presunzione d'innocenza e diritto di difesa*, in *Dir. pen. proc.*, 2014, p. 1409, secondo cui la facoltà di non autoincriminarsi ricomprende «il diritto di ogni cittadino di non fornire elementi che possano portare alla sua incriminazione, intesa come apertura di un procedimento a suo carico». Nello stesso senso, valorizzando la portata garantista dell'art. 6 CEDU, G. CANESCHI, *Il diritto a un processo equo*, in M. Ceresa-Gastaldo – S. Lonati (a cura di), *Profili di procedura penale europea*, Milano, 2023, p. 186; V. MANES – M. CAIANIELLO, *Introduzione al diritto penale europeo. Fonti, metodi, istituti, casi*, Torino, 2020, p. 251.

[62] È questa, in effetti, l'esegesi tradizionale offerta da V. GREVI, *Intercettazioni telefoniche e principi costituzionali*, in *Riv. it. dir. proc. pen*., 1971, p. 1068, per il quale la garanzia del diritto al silenzio «riguarda le sole ipotesi in cui l'inquisito si trova di fronte all'autorità (di polizia o giudiziaria), in posizione di più o meno marcata soggezione psicologica».

[63] V. GREVI, *Nemo tenetur se detegere*, cit., *passim*.

la garanzia del diritto al silenzio nell'attuale ordinamento»[64]. Com'è risaputo, le argomentazioni dell'illustre Autore sono state riprese dalla Corte delle Leggi allorquando, nell'anno successivo alla pubblicazione del manoscritto appena ricordato, fu rigettata una questione di legittimità costituzionale proprio con riferimento alla violazione degli artt. 15 e 24 Cost., nella parte in cui il mezzo di ricerca della prova risulta lesivo della facoltà di non autoincriminarsi[65]. In quel contesto, la Consulta ebbe modo di affermare che lo scopo della garanzia di derivazione anglosassone è quello di «rafforzare la libertà morale dell'imputato per sollevarlo dallo stato di soggezione psicologica in cui possa venire a trovarsi al cospetto dell'autorità e per porlo al riparo da eventuali pressioni che su di lui possano essere esercitate»[66]. Di conseguenza, nel caso di attività intercettativa, trattandosi di captazione fraudolenta di dichiarazioni spontanee verso un terzo interlocutore, non vi è alcun pericolo che la volontà del dichiarante possa essere inquinata o coartata dall'autorità procedente[67].

È in questa prospettiva, del resto, che si è sviluppato, a livello interno e sovranazionale, il fecondo dibattito relativo alla possibilità di imporre un obbligo legalmente sanzionato all'indagato (o a terzi) di svelare la *password* e le credenziali di accesso ai propri dispositivi elettronici. La questione verrà esaminata più dettagliatamente in seguito, ma ciò che preme rilevare in questa sede è, ancora una volta, la stretta contiguità che lega il *nemo tenetur se ipsum prodere* e la necessità che si vada instaurando, ai fini dell'attivazione della garanzia, una relazione dialogica e *de visu* tra l'indagato e l'autorità procedente.

Tornando all'esame della fattispecie che qui interessa, le considerazioni svolte fino a questo momento consentono di affermare l'assoluta estraneità del diritto contro l'autoincriminazione nel contesto della *false friends technique*[68]. Se, come detto, l'operatività di detta garanzia è subordinata alla presenza del dichiarante "al cospetto" dell'autorità, ne consegue che la polizia giudiziaria possa legittimamente acquisire con l'inganno dati ristretti presenti in un profilo *social* "semi-pubblico", senza che vi sia alcun rischio di veder coartata la volontà dell'utente. Egli, difatti, sceglie liberamente di

---

[64] V. GREVI, *Intercettazioni telefoniche e principi costituzionali*, cit., p. 1068.

[65] Cfr. Corte cost., 4 aprile 1973, n. 34, sulla quale, v., per tutti, V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1973, p. 317 ss.

[66] Cfr. Corte cost., 4 aprile 1973, n. 34, cit.

[67] In questo senso è orientata anche la dottrina maggioritaria: V. GREVI, *Intercettazioni telefoniche e principi costituzionali*, cit., p. 1067; O. MAZZA, *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, Milano, 2004, p. 53 ss.; G. ILLUMINATI, *La tutela della segretezza delle comunicazioni tra vecchio e nuovo codice*, in AA.VV., *Processo penale e valori costituzionali nell'insegnamento di Vittorio Grevi ad un anno dalla sua scomparsa*, Padova, 2013, p. 102; La giurisprudenza, sul punto, appare granitica: cfr. Cass., Sez. II, 12 giungo 2019, n. 37794; Cass., Sez. VI, 19 febbraio 2013, n. 16165; Cass., Sez. IV, 2 luglio 2010, n. 34807. Va detto, però, che a questo filone interpretativo si è vivacemente contrapposta un'autorevole corrente di pensiero che, seppur isolata, ha cercato di scardinare l'attuale sistema di diritto vivente mettendo in evidenza come la portata applicativa del diritto di non autoincriminarsi debba essere estesa anche con riferimento alle dichiarazioni autoaccusatorie captate occultamente attraverso lo strumento delle intercettazioni. In tali evenienze, infatti, il contributo conoscitivo apportato dall'imputato non sarebbe espressione di una libera e consapevole volontà di collaborare con l'autorità inquirente (cfr. A. GIARDA, *Dichiarazioni autoaccusatorie "intercettate" in conversazioni e comunicazioni*, in *Corr. mer.*, 2007, p. 11 ss.).

[68] *Contra*, M. TORRE, Open source intelligence: *spionaggio digitale e* social network, cit., p. 1717, per il quale, invece, «i dati (non comunicativi) "ristretti" ai c.d. "amici su *Facebook* ed appresi con l'inganno, pur non afferendo ad una collaborazione dichiarativa" del soggetto coinvolto nell'accertamento processuale, comportano un facere da parte di quest'ultimo, una sua collaborazione "attiva" e non "passiva", con tutto ciò che ne consegue con riferimento al principio del *nemo tenetur se detegere*».

condividere le proprie informazioni con terzi, nella piena in-consapevolezza del fatto che quella richiesta di "amicizia" proviene dall'autorità giudiziaria.

L'esclusione di possibili frizioni con il diritto a non autoincriminarsi, tuttavia, non sembra stemperare gli ulteriori aspetti problematici che potrebbero sorgere con specifico riguardo alla previsione dell'art. 188 c.p.p., a fronte di un'attività investigativa caratterizzata dalla presenza di un inganno digitale. Anche nel contesto delle indagini tecnologiche realizzate mediante l'impiego del "cavallo di troia", del resto, ci si è chiesti se l'utilizzo di tecniche che inducono surrettiziamente il *target*-indagato alla auto-installazione della "cimice elettronica" debba considerarsi lesivo della libertà di autodeterminazione.

La risposta al quesito, a ben considerare, è strettamente dipendente dalla nozione di "libertà morale" che si intende accogliere e dal rapporto tra quest'ultima e l'impiego di inganni e sotterfugi da parte dell'autorità investigativa[69]. Detto altrimenti, l'accettazione della richiesta di "amicizia" in modo volontario, ancorché non consapevole delle sue conseguenze sul piano processuale, può dirsi lesiva della libertà di autodeterminazione?

In questa prospettiva, il problema viene a collocarsi sul piano della (ir)rilevanza dell'inganno orchestrato dagli inquirenti ai fini dell'acquisizione probatoria. In effetti, l'utilizzo di sotterfugi e di tecniche subdole di acquisizione di dati e informazioni processualmente rilevanti è da sempre controverso e oggetto di ampio dibattito nella dottrina processuapenalistica[70]. Si pensi, ad esempio, al tema delle acquisizioni fraudolente del materiale biologico proveniente dall'indagato o, come accennato, all'impiego di tecniche occulte per indurre l'auto installazione del *trojan*. In entrambe le ipotesi, gli interpreti sono chiamati a stabilire se la condotta tenuta dall'indagato, indotta surrettiziamente dall'autorità inquirente, sia o meno lesiva della propria libertà morale.

A tal fine, è opportuno precisare che la soluzione al quesito – contrariamente a quanto sostenuto dalla giurisprudenza di legittimità – non si identifica tanto nel domandarsi se il cavallo di troia (o lo stratagemma orchestrato dagli agenti di polizia nel caso dell'acquisizione di materiale biologico) abbia o meno la capacità di alterale la genuinità del contenuto della conversazione o del comportamento non comunicativo captato o, ancora, del campione salivare raccolto[71]. È evidente, infatti, che l'autenticità dei dati e delle informazioni apprese non dipendono in alcun modo dal contegno tenuto dall'indagato. Anzi,

---

[69] In una prospettiva generale, ritiene che l'inganno orchestrato dalla polizia giudiziaria, comunque manifestato, sia sempre idoneo a incidere sulla libertà morale tutelata all'art. 188 c.p.p., L. FILIPPI, *Le Sezioni unite decretano la morte dell'agente segreto "attrezzato per il suono"*, in *Cass. pen.*, 2004, p. 2098. *Contra*, N. GALANTINI, voce *Vizi degli atti processuali penali*, *Dig. disc. pen.*, vol. XV, Torino, 1999, p. 364, per la quale l'errore generato dall'altrui inganno non comporta l'invalidità delle dichiarazioni eventualmente rese dall'indagato.

[70] Cfr., per un'accurata panoramica a livello internazionale e comparato, E.N. JONES, *The Good and (Breaking) Dad of Deceptive Police Practices*, in *New Mexico Law Review*, 2015, p. 523 ss.

[71] È questa la prospettiva adottata dalla Suprema corte in una recente sentenza nella quale si è affermato che «va escluso che il captatore informatico possa inquadrarsi tra "i metodi o le tecniche" idonei ad influire sulla libertà di determinazione del soggetto, come tali vietati dall'art. 188 cod. proc. pen.» dal momento che lo stesso «non esercita alcuna pressione sulla libertà fisica e morale della persona, non mira a manipolare o forzare un apporto dichiarativo, ma, nei rigorosi limiti in cui sono consentite le intercettazioni, capta le comunicazioni tra terze persone, nella loro genuinità e spontaneità» (Cass. pen., Sez. V, 30 settembre 2020, n. 31604).

è proprio il carattere ingannevole dell'operazione investigativa a costituire la più efficace conferma della genuinità del materiale probatorio acquisito[72].

Il punto, invece, è un altro. Occorre chiedersi se la condotta collaborativa, ma inconsapevole – poiché indotta con l'imbroglio –, realizzata dal *target* violi o meno la sua libertà di autodeterminarsi.

Le posizioni assunte dalla dottrina, come noto, sono varie e contrastanti.

Talvolta, il discrimine è stato individuato nella distinzione tra "collaborazione attiva" e "condotta passiva": è stato considerato legittimo, ad esempio, il prelievo fraudolento di campioni biologici, dato che quest'ultimo rappresenta un'attività subita (*pati*) dall'indagato senza richiedere una qualche forma di partecipazione proattiva[73]; così argomentando, per contro, si è negata con fermezza la possibilità di ricorrere al *trojan* nel caso in cui l'attività di "compromissione dell'*host*"[74] realizzata in maniera ingannevole richieda una qualche forma di *facere* in capo al *target*-indagato[75]. Talaltra, invece, la letteratura ha ritenuto corretta l'applicabilità dell'art. 188 c.p.p. solo con riguardo a quei mezzi di ricerca della prova rispetto ai quali viene a instaurarsi un rapporto dialogico, diretto e immediato tra l'indagato e l'autorità statale[76].

Con riguardo all'impiego di artifizi e raggiri per indurre in errore il cittadino e «costringerlo ad un atto che procura agli inquirenti l'"ingiusto profitto" di poterlo controllare»[77], però, il problema che si pone è, almeno in parte, differente. Più in dettaglio, occorre stabilire se l'impiego di pratiche surrettizie, ingannevoli e insidiose, in assenza di una relazione diretta e palese con l'autorità di polizia (che, nel caso della *social network false friends technique*, agisce sotto mentite spoglie), sia in grado di incidere sulla libertà di autodeterminazione e, dunque, di condizionare i comportamenti del bersaglio.

---

[72] Lo sottolineava, con riguardo alle captazioni telefoniche, già V. GREVI, *Intercettazioni telefoniche e principi costituzionali*, cit., p. 1068, per il quale l'attività intercettativa non incide sulla «libertà morale dell'inquisito», giacché questi è «normalmente ignaro di essere ascoltato».

[73] Per tale visione, v. S. SIGNORATO, *Le indagini digitali*, cit., p. 238.

[74] Questa è l'espressione tecnica utilizzata dagli ingegneri informatici per descrivere l'attacco informatico sferrato da *malware*.

[75] In questo senso sono orientati, ad es., M. BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont.*, 20 dicembre 2018, p. 14, per il quale «l'utilizzo del *virus* informatico non sarebbe praticabile nel caso in cui fosse accertata la lesione della libertà morale delle persone aventi la disponibilità del dispositivo elettronico portatile dove venga inoculato il captatore», come nel caso in cui «l'attività di inoculazione del trojan avvenga con l'inganno»; A. CHELO, *Tutela della libertà morale e captatore informatico: è davvero tutto concesso a soddisfazione delle esigenze investigative?*, in *Dir. pen. proc.*, 2022, p. 954 ss.; L. FILIPPI, *Ma davvero si può ricorrere a manovre fraudolente per intercettare col virus* trojan*?*, in *PenaleDP*, 9 febbraio 2021, secondo cui «non è ammissibile che lo Stato, al fine di reprimere le condotte illecite dei criminali, scenda al loro livello, ingannando l'indagato per indurlo a consentire inconsapevolmente l'accesso al "cavallo di Troia». Per una differente ricostruzione, v. M. MIRAGLIA, *Il "*Trojan *(non) di Stato": una disciplina da completare*, in *Proc. pen. giust.*, 2023, p. 1227 ss.

[76] Per questa opinione, v., in una prospettiva generale, N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Milano, 1992, p. 193; e, con specifico riguardo all'acquisizione di materiale biologico, P. FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Milano, 2007, p. 59; A. CAMON, *La disciplina delle indagini genetiche*, in *Cass. pen*., 2014, p. 1443, per il quale se la manovra investigativa «non implica un contatto con l'individuo (come nel caso dell'offerta maliziosa d'una bevanda o d'una sigaretta), allora l'eventuale inganno è irrilevante». *Contra*, però, C. FANUELE, *Dati genetici e procedimento penale*, Padova, 2009, p. 49.

[77] Così, benché con riguardo all'impiego del *trojan*, L. FILIPPI, *Il cavallo di Troia e l'ispe-perqui-intercettazione*, in *PenaleDP*, 21 marzo 2022, par. 5.

Viene in soccorso, a tal proposito, quanto contenuto nella Relazione al progetto preliminare del nuovo codice di rito, ove si afferma che l'obiettivo dell'art. 188 c.p.p. è quello di assicurare, «sull'intero fronte dei possibili interventi dell'autorità, la tutela della libertà morale del cittadino di fronte a mezzi coercitivi della volontà o a tecniche di subdola persuasione»[78]. L'impiego di quest'ultima locuzione sembra ricondurre nell'alveo delle attività lesive della libertà morale tutte quelle operazioni investigative che limitano o escludono *in toto* la facoltà della persona fonte di prova di determinarsi liberamente rispetto agli stimoli. Si allude, per riprendere le parole di autorevole dottrina, alla «libertà di ragionare con la propria testa […], la libertà di non vedere né ingannata né coartata la propria coscienza, il diritto a non vedersi ingiustamente imposto un determinato contegno, neanche passivo od inerte, il diritto infine […] a formare "con motivi propri le proprie determinazioni"»[79]. In questa prospettiva, dunque, il ricorso alle anzidette pratiche, «aggirando la volontà dell'individuo, influisce sulla formazione della medesima»[80].

Questo percorso esegetico muove da un'accezione ampia del concetto *de quo*, ricavabile dalla *littera* dell'art. 188 c.p.p., che presuppone la consapevolezza dell'interessato di essere coinvolto nell'esecuzione di un atto di indagine[81]. Da questo punto di vista, la libertà di autodeterminazione diviene lo strumento per assicurare che il soggetto sia pienamente cosciente e, soprattutto, consapevole della realtà circostante, giacché solo in tal modo la propria volontà potrà dirsi "formata" senza costrizioni, né intromissioni esterne. Evidente è l'approdo del discorso: l'invio di una richiesta di "amicizia" sotto mentite spoglie, prospettando una realtà difforme da quella effettiva, incide sulla libera determinazione della volontà. Le conseguenze, sul piano probatorio, sono radicali: il materiale acquisito deve considerarsi inutilizzabile.

Sennonché, il ricorso a un'interpretazione come quella appena ipotizzata potrebbe destare qualche riserva.

A ben riflettere, infatti, se il fine ultimo della disposizione codicistica è quello di vietare il ricorso a «ogni espediente psico-compulsivo»[82], non si comprende come il semplice utilizzo di un'identità fittizia possa incidere sul percorso di formazione della volontà. In questa prospettiva, ciò che occorre davvero garantire, onde rendere concreta la libertà di poter «determinare il proprio comportamento senza esterne imposizioni»[83], non è tanto la consapevolezza della realtà circostante, bensì la spontaneità del comportamento

[78] Relazione al progetto preliminare del codice di procedura penale, in Gazz. Uff., suppl. ord. n. 2, 24 ottobre 1988, Serie gen., p. 60.

[79] G. VASSALLI, *Il diritto alla libertà morale*, in *Scritti giuridici*, vol. III, *Il processo e la libertà*, Milano, 1997, p. 306 ss.

[80] C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, p. 163.

[81] Su questa linea di pensiero, seppur con riguardo al tema del prelievo "ingannevole" di reperti biologici, v. C. FANUELE, *Dati genetici e procedimento penale*, cit., p. 49. Questo approccio al tema sembra essere permeato dalle influenze di quella prospettiva esegetica che sostiene l'operare del *nemo tenetur se detegere* in tutti quei casi in cui l'indagato non ha piena consapevolezza che il suo apporto conoscitivo sarà utilizzato nel procedimento in corso (v. A. GIARDA, *Persistendo 'l reo nella negativa*, cit., p. 9).

[82] F. CORDERO, *Procedura penale*, Milano, 2012, p. 616.

[83] Questa è la definizione di "libertà morale" offerta da G. VASSALLI, *Il diritto alla libertà morale*, cit., p. 289. In termini non dissimili, v. anche V. PATANÈ, *Il diritto al silenzio dell'imputato*, Torino, 2006, p. 102, ove definisce tale concetto come «libertà del singolo […] di agire in conformità alle spinte psichiche interne».

collaborativo, ovverosia l'assenza di un impulso esterno idoneo a influire sul processo decisionale.

Esemplificativo, ancora un vola, si rivela il caso dell'impiego del *trojan* di Stato. Si è detto che la compromissione dell'*host* può avvenire attraverso l'impiego di tecniche più o meno invasive della sfera privata del bersaglio. La prassi giudiziaria, infatti, dimostra che, qualora i tentativi di inoculazione promossi dall'autorità inquirente non vadano a buon fine, si individuano stratagemmi ulteriori, arrivando financo a bloccare le chiamate in entrata e in uscita dal *device*[84]. Ebbene, in quest'ultima ipotesi viene inibito l'esercizio del diritto fondamentale alla comunicazione, realizzandosi così – a differenza di quanto sembra prospettarsi con riguardo alla *false friends technique* – una sorta di "coercizione indiretta" idonea a influire sulla formazione della volontà e, di conseguenza, sulla libertà morale del *target*. In questo caso, all'utente non è garantito – per utilizzare un linguaggio proprio degli studiosi di diritto penale sostanziale – il concreto esercizio di "un'alternativa comportamentale", cosicché egli è indirettamente costretto alla auto installazione del *virus*.

In queste coordinate teoriche, pertanto, risulta chiaro come la sollecitazione (si legga, l'invio di una richiesta di "amicizia") mediante il ricorso a un'operazione *lato sensu undercover* non incida in alcun modo sulla autonoma determinazione dell'agire, cioè sulla «libertà di ragionare con la propria testa»[85]; in fin dei conti, «ad assicurare il successo di [queste] strategie inquirenti è […] un comportamento liberamente tenuto»[86].

Ad abundantiam, non è fuor d'opera sottolineare come, proprio accogliendo questa prospettiva, parte della dottrina, per converso, abbia criticato l'impiego a fini investigativi degli agenti segreti attrezzati per il suono. A prescindere dal fatto che la registrazione venga eseguita da un funzionario pubblico o da un privato che agisce d'intesa con la polizia giudiziaria, un dato parrebbe inconfutabile: l'indagato – colloquiante ignaro – terrà un contegno manipolato, anche involontariamente, da colui che effettua la registrazione[87]. Benché il confine tra il tra il «percepito e il provocato» appaia assai evanescente[88], è facile ipotizzare che l'agente attrezzato per il suono abbia interesse a condurre la conversazione in modo tale da carpire dichiarazioni a sé favorevoli. Per siffatta ragione, la relazione dialogica che viene a instaurarsi tra l'autorità (sotto mentite spoglie) e il dichiarante incide sulla manifestazione di volontà e sul processo volitivo del colloquiante ignaro. Valorizzando

[84] M. MIRAGLIA, *Il "*Trojan *(non) di Stato"*, cit., p. 1233.

[85] Così, ancora, G. VASSALLI, *Il diritto alla libertà morale*, cit., p. 306.

[86] Testualmente, benché in altro contesto, C. GABRIELLI, *Il prelievo coattivo di campioni biologici nel sistema penale*, Torino, 2012, p. 16. Concorde A. CAMON, *La disciplina delle indagini genetiche*, cit., p. 1443. Anche F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. Bras. de Direito Processual Penal*, 2017, p. 486, ancorché con riferimento all'inoculazione fraudolenta del *trojan*, ritiene che «l'utilizzo del *virus* informatico non sembra inoltre in grado di "pregiudicare la libertà morale" (*id est*, di condizionare i comportamenti) delle persone coinvolte nell'indagine». Nello stesso senso, v. M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017, p. 69, per il quale il carattere subdolo del captatore costituirebbe la miglior garanzia della integrità del processo volitivo della persona.

[87] P. GAETA, *Dichiarazioni dell'indagato "provocate" da agenti infiltrati: la libertà di autodeterminazione quale canone di utilizzabilità*, in *Cass. pen.*, 2000, p. 974, parla di una «manipolazione narrativa» delle parole dell'indagato. Sul punto, cfr., volendo, A. MALACARNE, *Le registrazioni di colloqui ad opera di uno degli interlocutori tra contrasti interpretativi ed evoluzione tecnologica*, in *Dir. Internet*, 2021, p. 159 ss.

[88] P. GAETA, *Dichiarazioni dell'indagato "provocate" da agenti infiltrati*, cit., p. 975.

l'elemento della spontaneità delle dichiarazioni rese dall'indagato, dunque, si è ragionevolmente sostenuta l'inutilizzabilità processuale di quest'ultime per violazione dell'art. 188 c.p.p.[89].

6. Il concetto di "*privacy* interpersonale" quale limite all'impiego degli *undercover social network accounts*

A fronte di un dato normativo poco chiaro (art. 188 c.p.p.) e un'interpretazione dottrinale oscillante e non univoca con riguardo al concetto di libertà di autodeterminazione, il baricentro dell'analisi parrebbe doversi orientare sul versante della tutela dei diritti fondamentali e, in specie, del diritto alla riservatezza e al rispetto della vita privata. Laddove si dimostri, come si cercherà di fare in questa sede, che la *false friends technique* incide sulla garanzia prevista all'art. 8 CEDU, se ne dovrebbe dedurre – in mancanza, *de iure condito*, di una legge che disciplina casi e modi dell'intrusione – l'inutilizzabilità del materiale acquisito. L'art. 189 c.p.p., come si è già osservato in relazione all'impiego del *cyberpatrolling*, non costituirebbe una base legale idonea a legittimare l'intrusione nella sfera privata del cittadino[90].

Si proceda con ordine.

È opinione ricorrente – lo si è detto – che la mera richiesta di *follow* inoltrata su un *social network* dalla polizia giudiziaria che agisce sotto mentite spoglie non incida in alcun modo sulla aspettativa di riservatezza vantata dal bersaglio. Del resto, l'ipotesi *de qua* non risulta poi così diversa dal caso in cui un agente in borghese riesca ad accedere con l'inganno nell'abitazione dell'indagato. Pure la giurisprudenza nordamericana, ad esempio, è granitica nell'afferma che le forze dell'ordine, ancorché in assenza di un *warrant*, possono utilizzare artifici e raggiri atti a manipolare il consenso dell'indagato per introdursi nel suo domicilio – al pari di quanto potrebbe fare un privato cittadino – al fine di carpire dati e informazioni riservate[91].

Il paragone, però, genera qualche perplessità.

Innanzitutto, la polizia giudiziaria, nell'ipotesi di accesso fraudolento in un luogo di privata dimora riconducibile all'imputato, è costretta, gioco forza, a entrare in contatto diretto con quest'ultimo; un'attività relazionale che, come si è visto, non viene espletata nel caso della mera richiesta di *follow* sui *social network*. Inoltre, mentre l'accesso "fisico" consente agli investigatori di apprendere esclusivamente dati e informazioni esistenti in *rerum natura* fino a quel momento, l'impiego della *false friends technique*, per contro, attribuisce all'autorità statale la possibilità di acquisire tutto ciò che è, è stato e sarà pubblicato dal bersaglio nel corso della propria "vita digitale".

---

[89] Per questa opinione, v. F.R. DINACCI, *L'irrilevanza processuale delle registrazioni di conversazioni tra presenti*, in *Giur. it.*, 1994, p. 1 ss.; L. LUPÁRIA, *La confessione dell'imputato nel sistema processuale penale*, cit., p. 174.

[90] Più in generale, sull'impossibilità di invocare il disposto dell'art. 189 c.p.p. per giustificare l'impiego di strumenti investigativi atipici, v., da ultimo, S. SIGNORATO, *Rimodulazioni normative dell'uso investigativo del captatore informatico*, in G. Giostra – R. Orlandi (a cura di), *Revisioni normative in tema di intercettazioni. Riservatezza, garanzie difensive e nuove tecnologie*, Torino, 2021, p. 323.

[91] *Florida c. Jardines*, 133 S. Ct. 1409, 1416 (2013).

Al netto di tali aspetti (tutt'altro che irrilevanti), ciò che non convince affatto è l'idea – sottesa all'esegesi in esame – che il concetto di *privacy* debba collocarsi in una dimensione squisitamente individuale ed essere interpretato, perciò, come un mero diritto alla tutela delle proprie informazioni a carattere segreto e riservato. A ben vedere, invece, la riservatezza non è soltanto un valore primario di carattere personale, ma costituisce, altresì, un fondamentale bene collettivo destinato ad assumere una valenza pubblico-relazionale.

Il tema, per la centralità che assume ai fini dell'analisi, merita di essere approfondito.

Tradizionalmente, la letteratura tende a contrapporre la dimensione individuale propria della riservatezza («*right to be let alone*»[92]) con la portata sociale e collettiva della vita pubblica[93]. D'altro canto, la *privacy* nasce proprio con l'obiettivo di delineare una netta linea di confine tra ciò che è riservato e ciò che è di dominio comune, enucleandosi in tal modo un vero e proprio «*rights as against the world*»[94], ovverosia uno spazio individuale nel quale lo Stato e gli altri cittadini non possono accedere. Epperò, non è difficile scorgere nella *privacy* anche una vocazione sociale e collettiva, dal momento che la capacità degli individui di controllare chi ha accesso ai propri dati (*habeas data*) consente di mantenere una varietà di rapporti con gli altri, travalicando così una dimensione squisitamente individuale e assumendo, per contro, una valenza pubblico-relazionale. La riservatezza, da questo punto di vista, non riguarda soltanto «"il giardino segreto" entro il quale l'individuo vorrebbe vivere la propria vita al riparo dall'altrui indiscrezione», bensì anche «la tutela del bisogno, che lo stesso individuo avverte, di uscire, a volte, da quel "giardino segreto" per partecipare certi aspetti di sé stesso ad altri»[95]. Una prospettiva, quest'ultima, che, a ben pensare, si ricollega a quell'idea aristotelica – richiamata in apertura della presente trattazione – di essere umano come "animale sociale", cioè un individuo che, pur avendo necessità di mantenere segreta la propria intimità, vive in un contesto caratterizzato da legami intersoggettivi.

Preso atto, dunque, dell'esistenza di una componente "pubblico-relazionale" e "sociale" della *privacy*, è agevole comprendere la ragione per la quale la Corte di Strasburgo ha ricondotto all'art. 8 CEDU la tutela di quello che si potrebbe definire un vero e proprio "diritto a stabilire, sviluppare e coltivare relazioni libere e consapevoli con altri esseri umani"[96]. I giudici, dopo aver precisato a più riprese che il concetto di "vita privata" «*is a broad term not susceptible to exhaustive definition*», hanno sottolineato come tale locuzione non debba essere interpretata in senso restrittivo, cioè come diritto individuale a escludere terzi dalla propria sfera di intimità (si legga, «*le droit de vivre en privé, loin de toute attention non voulue*»). Trattasi, al contrario, di un diritto sì di natura individuale, ma a vocazione collettiva, diretto a garantire a chiunque la possibilità di definire liberamente e, soprattutto,

---

[92] Secondo la nota definizione offerta dai "padri" della *privacy*, S. WARREN – L. BRANDEIS, *The Right to Privacy*, in *Harward Law Review*, 1890, 4, p. 193.

[93] V. STEEVES, *Reclaiming the Social Value of Privacy*, in I. Kerr, V. Steeves y C. Lucock (a cura di), *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*, New York, p. 191 ss.

[94] S. WARREN – L. BRANDEIS, *The Right to Privacy*, cit., p. 213.

[95] Così, nel cogliere la portata "relazionale" della *privacy*, M. PISANI, *La tutela penale della «riservatezza»: aspetti processuali*, in *Riv. it. dir. proc. pen.*, 1967, p. 798.

[96] Cote edu, *Niemietz c. Germania*, 16 dicembre 1992, par. 29. Più di recente, Corte edu., *P.G. e J.H. c. Regno Unito*, 25 dicembre 2001, par. 56.

consapevolmente, le proprie relazioni sociali (*rectius*, «*le droit de mener une "vie privée sociale"*»[97]).

In questo senso, la riservatezza va assumendo una valenza di tipo relazionale: si potrebbe fare riferimento, in proposito, a una forma di "*privacy* interpersonale", intesa quale diritto del singolo cittadino di instaurare e costruire legami sociali puri, sinceri, consapevoli e liberi da intrusioni statali, inibendo così alle autorità pubbliche di interferire con gli aspetti essenziali di una relazione umana. Come riconosciuto dalla stessa Corte Suprema americana nel famoso caso *Lawrence c. Texas*[98], il IV emendamento è volto a tutelare non solo la *privacy* dei cittadini nella sua dimensione individuale, ma anche le sue numerose articolazioni come presupposto per l'instaurazione di rapporti intersoggettivi[99].

Le considerazioni svolte fino a questo momento assumono una valenza ancor maggiore se trasposte nella realtà digitale[100]. I numerosi studi psicologici, sociali e giuridici[101] che hanno esaminato la natura e la tipologia di connessioni che si instaurano nel contesto dei *social network* avallano la tesi di un'equivalenza qualitativa rispetto ai rapporti umani costruiti e coltivati "faccia a faccia" nel mondo analogico. Se un tanto è vero, la garanzia prevista all'art. 8 CEDU sembra essere destinata a trovare applicazione anche con riguardo ai legami interpersonali che si vanno instaurando in contesti digitali. Di conseguenza, l'attività investigativa volta ad acquisire con tranelli e sotterfugi il contatto dell'indagato, risolvendosi in un tentativo di stabilire una qualche forma di relazione sociale, incide sul diritto a sviluppare e coltivare liberamente – nonché, consapevolmente – le proprie relazioni interpersonali.

Se ne ricava, sul piano *stricto sensu* processuale, la necessità che simili attività siano subordinate alla previsione di una legge chiara e precisa che individui casi e modi dell'intrusione, nonché a un'autorizzazione adottata da un'autorità terza e imparziale. Sennonché, in assenza di una disciplina *ad hoc*, vengono a riproporsi le considerazioni già spese nei capitoli precedenti con riguardo alle operazioni di *cyberpatrolling* occulto e continuativo[102]: inutilizzabilità, *de lege lata*, del materiale acquisito e indispensabilità, *de iure condendo*, di un intervento legislativo volto a individuare limiti e procedure per la realizzazione di queste operazioni investigative.

In conclusione, sembra potersi affermare che le problematiche sottese all'impiego di tecniche fraudolente e dissimulate ai fini dell'acquisizione di materiale probatorio presente nelle *web communities* chiamino direttamente in causa il rapporto Stato-individuo.

---

[97] Così, per le ultime citazioni, Corte edu, 28 maggio 2009, *Bigaeva c. Grecia*, par. 22.

[98] *Lawrence v. Texas*, 539 U.S. 558 (2003).

[99] T.C. CROCKER, *From Privacy to Liberty: The Fourth Amendament after Lawrence*, in *UCLA Law Review*, 2009, p. 56.

[100] Sul punto, si vedano le interessanti riflessioni offerte da I. TURÉGANO MANSILLA, *La dimensión social de la privacidad en un entorno virtual*, in AA.VV., *Era Digital, Sociedad Y Derecho*, Valencia, 2020, p. 27 ss.

[101] J. GRIMMELMANN, *Saving Facebook*, in *Iowa Law Review*, 2009, p. 1137 ss., spec., p. 1151 ss.; M. BEDI, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should not Apply*, in *Boston College Law Review*, 2013, p. 51, nt. 387 e, p. 53-55, al quale si rinvia per un ampio richiamo bibliografico. Anche la giurisprudenza europea ha riconosciuto che i *social network* sono «una delle forme di comunicazione che permettono alle persone di condurre una vita sociale privata» (Corte edu, 5 settembre 2017, *Bărbulescu c. Romania*, par. 71).

[102] Cfr. Parte II, Cap. II.

Nell'attuale contesto delle indagini penali, non appare ragionevole esigere che detta relazione sia sempre e comunque incentrata su un principio di lealtà[103]. Negare all'autorità inquirente la possibilità di ricorrere a inganni, sotterfugi e tecniche *lato sensu undercover* significherebbe ostacolare gravemente l'*iter* di accertamento dei fatti. Tuttavia, se è vero, com'è vero, che occorre trovare un punto di equilibrio tra il principio di persecuzione penale e i diritti fondamentali dei soggetti indagati, non può dubitarsi del fatto che il vero nodo da sciogliere riguardi le condizioni, i limiti e le procedure da seguire nello svolgimento di questa nuova tecnica di indagine 2.0.

7. Le "amicizie *online*" come fonte indiretta di informazioni: il caso del "*follower* cooperante"

La lista degli amici o dei *followers* di un utente dei *social network* è spesso pubblica e, perciò, accessibile a chiunque. In tale evenienza, la polizia giudiziaria, al pari di ogni cibernauta, ben potrebbe individuare e contattare un cd. *target's friends* (*rectius*, un "amico" o *follower* dell'indagato) onde convincerlo a collaborare, al fine di acquisire dati e informazioni ristrette presenti sul profilo dell'indagato e, eventualmente, per "pattugliare", in nome e per conto dell'autorità, i movimenti digitali del bersaglio.

Al netto del differente *modus adoperandi* utilizzato dalle forze dell'ordine – che, dal punto di vista dogmatico, appare, come si vedrà, del tutto irrilevante –, potrebbe teoricamente sostenersi che l'operazione *de qua agitur* debba essere ricondotta nel novero di quelle attività liberamente espletabili dalla polizia giudiziaria, pur in assenza di un *placet* giudiziale (artt. 55, 348 e 370 c.p.p.). A supporto di tale conclusione soccorrerebbe la già richiamata "teoria dell'accettazione del rischio" che costituisce, a tutti gli effetti, uno dei corollari della *Third party doctrine*. Più nel dettaglio, potrebbe affermarsi che la diffusione volontaria di informazioni a più persone porti con sé l'accettazione del rischio che queste possano, in seguito, utilizzarle come meglio credono, ben potendo anche trasmetterle alle forze dell'ordine[104]. Come si è efficacemente osservato, un individuo, specialmente nel contesto delle piattaforme digitali, non può avere «*a privacy interest in the loyalty of his friends*»[105].

In questa prospettiva, le informazioni ristrette dovrebbero ritenersi legittimamente acquisibili dalla polizia giudiziaria, poiché apprese – in assenza di manovre occulte o sotterfugi – da un soggetto ("l'amico intermediario") che ne aveva libera disponibilità. Nessuna violazione della riservatezza può essere, dunque, invocata[106]. Onde rendersi conto

[103] Si mostrano critici, invece, su questa modalità "non etica" di acquisizione del materiale probatorio (si legga, acquisizione con l'inganno), con specifico riferimento all'impiego del *trojan*, A. CHELO, *Tutela della libertà morale e captatore informatico*, cit., p. 954; L. FILIPPI, *Ma davvero si può ricorrere a manovre fraudolente per intercettare col* virus trojan*?*, cit., par. 2, per il quale «non è ammissibile che lo Stato, al fine di reprimere le condotte illecite dei criminali, scenda al loro livello, ingannando l'indagato per indurlo a consentire inconsapevolmente l'accesso al "cavallo di Troia"»; e, in relazione al caso qui in esame, M. TORRE, Open source intelligence: *spionaggio digitale e* social network, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 1718.

[104] Cfr. C. WARKEN, *Classification of Electronic Data for Criminal Law Purposes*, in *Eucrim*, 2018, 4, p. 3 ss.

[105] D.L. SLOVE – P.M. SCHWARTZ, *Privacy, Law Enforcement, and National Security*, Aspen, 2015, p. 18.

[106] Non rilevano alcuna violazione della *privacy*: E.E. NORTH, *Facebook Isn't Your Space Anymore*, cit., p. 1279 ss.; M. BEDI, *Facebook and Interpersonal Privacy*, cit., p. 62 s.; P. TROISI, *Le investigazioni digitali sotto*

di ciò, sarebbe sufficiente richiamare il contenuto della *privacy policy* di una tra le più diffuse piattaforme di comunicazione digitale. Nelle regole di condotta adottate da *Facebook*[107], infatti, si stabilisce che gli utenti dovrebbero essere consapevoli del fatto che le informazioni diffuse sulla propria pagina personale, ancorché con modalità tali da restringere la platea dei possibili destinatari, potrebbero essere condivise o ri-pubblicate da altri cibernauti. Di conseguenza, il *provider* non può in nessun caso «garantire che le informazioni condivise […] non diventino di dominio pubblico». In tali evenienze, vi è, in effetti, un'oggettiva difficoltà nel controllare la circolazione dei propri dati ristretti; ma tutto ciò, d'altro canto, non è nient'altro se non la evidente e scontata conseguenza della principale caratteristica dei *social network*: la cronaca permanente della vita delle persone.

L'assunto che si va esponendo, peraltro, parrebbe confermato in numerose pronunce in materia adottate dalle corti americane. I giudici d'oltreoceano, infatti, hanno più volte sottolineato come la polizia giudiziaria possa accedere ed esaminare liberamente le informazioni digitali ristrette ottenute grazie alla cooperazione di chi sia già "amico virtuale" del bersaglio. Esemplificativo è, al riguardo, il *leading case Stati Uniti c. Meregildo*, avente ad oggetto un caso nel quale l'autorità inquirente è riuscita a ottenere una grande mole di dati grazie alla collaborazione di un *follower*. La corte, pur riconoscendo che il grado di tutela della riservatezza vantato dal singolo utente varia a seconda delle impostazioni di *privacy*, ha affermato che l'indagato non avesse alcuna giustificabile e ragionevole aspettativa di riservatezza sul fatto che i suoi amici mantenessero riservate quelle informazioni. E, del resto, è proprio l'idea che gli individui utilizzino i *social network* allo scopo di connettersi con altri che espone consapevolmente i propri dati a una diffusione potenzialmente incontrollabile. Per tale ragione, laddove le impostazioni di *privacy* adottate dall'utente consentano a terzi di visualizzare i *post* presenti nella propria pagina personale, questi ultimi sono liberi di utilizzarle come meglio credono, financo condividendole con le autorità governative. In questi casi, conclude la Corte, «*[the defendant's] legitimate expectation of privacy ended when he disseminated posts to his "friends"*»[108].

Le linee argomentative delle quali si è dato conto fino a questo momento, però, non possono essere condivise.

In particolare, la circostanza che l'acquisizione occulta sia realizzata da un soggetto privato che aveva libero accesso alle informazioni ancor prima di assumere il ruolo di "agente sotto

---

copertura, cit., p. 322. *Contra*, in una più condivisibile prospettiva, M. O'FLOINN – D. ORMEROD, *Social Networking Sites, RIPA and Criminal Investigations*, in *Criminal Law Review*, 2011, p. 781.

[107] FACEBOOK, *Privacy Policy*. Su questo aspetto, v. L.M. GLADYSZ, *Status Update: When Social Media Evidence Enters the Courtroom*, in *Journal of Law and Policy for the Information Society*, 2012, p. 716.

[108] *Stati Uniti c. Meregildo*, 2012, 883 F. Supp. 2d, 526. Conformi, tra le molte, *Palmieri c. Stati Uniti*, 72 F. Supp. 3d 191, 210 (D.D.C. 2014), ove si afferma che, quando un utente di *Facebook* consente ai propri "amici" di visualizzare le proprie informazioni, il governo può accedervi «*throught an individua who is a friend without violating the Fourt Amendamet*»; *Rosario c. Clark City Sch. Dist*., No. 2:13-CV-362 JCM (PAL), 2013 WL 3679375 (D. Nev. 3 luglio 2013): «*when a person twiets on Twetter to his or her friends, that persona take the risk that the friend will turn the information over the government*»; *Everett c. State*, 186 A3d 1224 (Del. 2017); *Stati Uniti c. Devers*, 2012WL 12540235. In dottrina, nella medesima prospettiva, anche con riguardo all'ipotesi in cui gli "amici" del bersaglio consegnino direttamente le *password* dei propri profili alle autorità investigative al fine di acquisire i dai ristretti, M.J. HODGE, *The Fourth Amendament*, cit., p. 112 s., per il quale laddove i «*friends consent to allowing the police to see the information, then an expectation of privacy is destroyed*»; T.A. HOFFMEISTER, *Social Media in the Courtroom*, cit., p. 77.

copertura" appare assolutamente inconferente al fine di valutare un'eventuale lesione arrecata al diritto alla riservatezza. Per rendersi conto di ciò, è sufficiente richiamare, ancora una volta, le problematiche interpretative sorte in tema di "agente segreto attrezzato per il suono", con specifico riferimento al caso in cui l'operazione sia realizzata, nel corso del procedimento penale, da un privato non appartenente alle forze dell'ordine (come, ad esempio, la vittima o un terzo collaboratore). Laddove egli si muova d'intesa o su impulso dell'autorità giudiziaria, sembra possibile sostenere l'instaurarsi di una sorta di "identità sostanziale" fra quest'ultimo e l'autorità investigativa, giacché egli agisce, seppur informalmente, nella veste di organo d'accusa o, meglio, quale sua *longa manus*. Ancorché, in tali ipotesi, il rapporto tra polizia giudiziaria e indagato risulti, per così dire, "mediato" dalla presenza di un terzo, la circostanza che il cittadino agisca "in nome e per conto" del potere statale sembra giustificare una vera e propria "procedimentalizzazione" dell'atto, ovverosia la sua riconducibilità all'autorità inquirente[109].

Trattasi di considerazioni che, a ben vedere, possono essere spese anche con riguardo al tema che ci occupa. Gli inquirenti, sfruttando la collaborazione di un soggetto privato, l'"amico virtuale intermediario", procedimentalizzano l'atto che, di conseguenza, risulta in tutto e per tutto a loro riferibile. Cosicché, una volta ricondotta questa attività nell'ambito delle operazioni di polizia, possono esser offerte pure in questa sede le considerazioni già svolte nel paragrafo precedente in relazione alla violazione, *de lege lata*, dell'art. 8 CEDU. Un intervento legislativo appare, anche in seno a detta ipotesi, assolutamente indispensabile.

8. Investigazioni difensive e acquisizione di "dati ristretti"

L'avvento delle nuove piattaforme di comunicazione ha inciso notevolmente non solo sullo svolgimento delle attività di polizia preventiva e repressiva, ma, altresì, sui poteri investigativi attribuiti dal codice di procedura penale al difensore e ai suoi collaboratori[110]. Anche l'esercizio del diritto di difesa, infatti, è stato influenzato – e lo sarà sempre di più – dall'avvento dei *social network*, specialmente con riguardo al cd. "diritto di difendersi cercando", ricavabile dagli artt. 24, comma 2 e 111, comma 3, Cost.

È in tale prospettiva che si colloca il dibattito recentemente sviluppatosi nel contesto nordamericano in merito alle implicazioni etico-giuridiche dell'impiego delle piattaforme di *sharing*. Tra le questioni più interessanti oggetto di attenzione in letteratura può essere senz'altro annoverata proprio quella relativa all'impiego di *fake profiles* da parte dell'avvocato, al fine di acquisire informazioni altrimenti inaccessibili. Sono in costante crescita, d'altro canto, anche nel panorama italiano, i casi in cui i patrocinanti e gli investigatori privati autorizzati creano un "falso profilo" utilizzando nomi e immagini di fantasia o identità riconducibili a persone terze, nella speranza che il *target* individuato (possibile testimone, vittima, etc.) accetti la richiesta di "contatto", consentendo così l'ingresso ai propri dati ristretti. Se non appare dubitabile che il difensore (o un suo delegato)

[109] Per questa opinione, v. C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., p. 308.

[110] Per una panoramica, v. K. MINOTTI, *The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, in *South Carolina Law Review*, 2009, p. 1057 ss.

possa acquisire liberamente e senza limiti quantitativi o temporali i dati *open access* presenti su una "pagina pubblica", più complesso è, per contro, stabilire se e come sia consentito ricorrere a tecniche ingannevoli e fraudolente per ottenere informazioni che l'utente ha scelto di mantenere private.

8.1 I limiti deontologici: brevi cenni

Dal punto di vista deontologico, il tema, a differenza di quanto è dato rilevare nel panorama italiano, ha dato vita a un ampio dibattito all'interno dei Comitati etici dell'avvocatura d'oltreoceano[111].

Il *New York City Bar Committee on Professional Ethics*, ad esempio, è stato chiamato a stabilire se un avvocato, agendo personalmente o per il tramite di un investigatore privato, possa ricorrere a un inganno via *Internet* per ottenere l'accesso a un profilo *social* altrimenti precluso. Il comitato, dopo aver escluso qualsivoglia rilevanza disciplinare del mero invio di una richiesta di "amicizia" utilizzando identità "non fittizie", ha stabilito che debba ritenersi vietata la condotta del difensore (o dell'investigatore a ciò autorizzato) che ricorra a stratagemmi o sotterfugi per ottenere informazioni da un utente dei *social network*, giacché tale condotta appare in contrasto con la regola del Codice deontologico che vieta al patrocinante di tenere comportamenti disonesti e ingannevoli nei confronti di terzi[112].

La conclusione è stata confermata in successive pronunce disciplinari, nelle quali si è sottolineato come tale divieto è destinato a trovare applicazione indipendentemente dal fatto che la persona a cui si chieda l'"amicizia" sia già rappresentata da un altro avvocato o sia, lei stessa, parte in causa[113]. L'assunto, peraltro, risulta avvalorato pure dalla lettura dell'*American Bar Assosiation's Model Rules of Professional Conduct*, il cui art. 8, comma 1, lett. c), qualifica in termini di «*misconduct*» la condotta dell'avvocato che implichi disonestà, frode, inganno o false dichiarazioni. Non v'è dubbio, da questo punto di vista, che l'impiego di artifizi e raggiri che si sostanzino nell'utilizzo di identità *online* fittizie sia riconducibile a un comportamento eticamente censurabile.

Ancorché non si rivengano precedenti simili sul versante nazionale, sembrerebbe potersi argomentare nel senso che l'invio di una richiesta di *follow* da un profilo falso violi le generali regole di condotta previste dal Codice deontologico forense e dalla legge professionale.

Quest'ultima, in dettaglio, stabilisce che l'avvocato debba esercitare il proprio incarico con «indipendenza, lealtà, probità, dignità, decoro, diligenza e competenza» (art. 3, comma

---

[111] Per uno sguardo d'insieme, cfr. S. WITNOV, *Investigating Facebook: The Ethics of Using Social Networking Websites in Legal Investigations*, in *Santa Clara Computer Law & High Technology Law Journal*, 2011, p. 31 ss.; M.B. FLEMING – J.T. WELLS, *Ethical, Evidentiary, and Constitutional Concerns of Utilizing Social Networking Web Sites in Civil and Criminal Cases: the Good, the Bad, and the Ugly*, in *Southern Law Journal*, 2010, p. 23 ss.; M. O'FLOINN – D. ORMEROD, *Social Networking Material as Criminal Evidence*, in *Criminal Law Review*, 2012, p. 486 ss. e, spec., p. 510 s.

[112] NEW YORK CITY BAR COMMITTEE ON PROFESSIONAL, *Formal Opinion 2010-02: Obtaining Evidence From Social Networking Websites*, 9 ottobre 2010. Nello stesso senso, v. le opinioni rese dal PHILADELPHIA BAR ASSOCIATION, *Professional Guidance Committee issued Opinion 2009-02*; Corte Suprema del New Jersey, *Disciplinary Review Board*, 30 aprile 2020.

[113] SAN DIEGO COUNTY BAR ASSOCIATION, *Legal Ethics Opinion 2011-2*.

2, l. 31 dicembre 2012, n. 247). Il richiamo alla lealtà e alla correttezza nell'espletamento del mandato difensivo, inoltre, è espressamente previsto agli artt. 9, comma 1 e 63, comma 2 delle "norme etiche", laddove si stabilisce che il difensore debba tenere un comportamento «corretto» e rispettoso nei confronti dei propri dipendenti, del personale giudiziario e, per quel che più interessa, «di tutte le persone con le quali venga in contatto nell'esercizio della professione». Quantunque le norme deontologiche non vietino espressamente – a differenza di quanto previsto dall'*American Bar Assosiation* – comportamenti fraudolenti o ingannevoli, il riferimento ai concetti di «correttezza», lealtà e «onestà» nei rapporti con terzi sembrerebbe deporre nel senso dell'"immoralità" della condotta in esame. Senza voler considerare, in aggiunta, che, come già ricordato, l'impiego di un profilo *fake* implica una vera e propria violazione dei termini contrattuali che l'utente è chiamato a sottoscrivere al momento dell'ingresso nella *social network community*.

8.2 I limiti normativi

La legge 7 dicembre 2000, n. 397, come noto, ha introdotto nell'ordinamento italiano il titolo VI-*bis* del libro quinto del codice di procedura penale che ha finalmente approntato una disciplina organica in tema di investigazioni difensive. Si è definitivamente superato, in tal modo, il vecchio sistema imperniato sull'art. 38 disp. att. c.p.p. che riconosceva al difensore dell'indagato e della persona offesa la «facoltà di svolgere indagini per ricercare e individuare elementi di prova a favore del proprio assistito». La nuova regolamentazione ha cercato di realizzare quell'auspicata "parità delle armi" in sede di indagine, presupposto necessario per rendere davvero effettivo quello che è stato incisivamente definito "diritto alla prova". Un sistema a vocazione accusatoria, del resto, non poteva che consentire a tutte le parti – e, dunque, anche alla difesa – di svolgere attività di ricerca finalizzate ad acquisire informazioni processualmente rilevanti[114].

Tanto premesso, è necessario anzitutto stabilire se l'attività di *false friends technique* possa essere ricondotta a uno degli atti tipizzati agli artt. 391-*bis* ss. c.p.p. L'attenzione, da questo punto di vista, sembrerebbe doversi orientare, in via esclusiva, alla disciplina dell'«accesso ai luoghi privati o non aperti al pubblico» di cui all'art. 391-*septies* c.p.p. La disposizione, come risaputo, stabilisce che, qualora risulti necessario accedere a luoghi diversi da quelli pubblici[115], il difensore debba ottenere il consenso di chi ne ha la disponibilità; solo in caso di diniego esplicito, egli potrà rivolgersi al giudice per essere a tale scopo autorizzato.

Ebbene, il ricorso a un'interpretazione estensiva del concetto di "luogo" potrebbe far propendere per la riconducibilità della *false friends technique* nell'ambito del menzionato articolo, dal momento che il profilo *social* chiuso (*restricted profile*) sembrerebbe in tutto e per tutto equiparabile a un luogo "non aperto al pubblico", per il cui accesso è richiesto il consenso del legittimo titolare.

Un'esegesi di questo tipo, però, genera più di qualche perplessità.

---

[114] È solo all'inizio del nuovo millennio, dunque, che si è faticosamente realizzato un vero e proprio passaggio «dal diritto di difendersi provando al diritto di difendersi cercando» (A. GIARDA, *Un cammino appena iniziato*, in AA.VV., *Le indagini difensive. Legge 7 dicembre 2000, n. 397*, Milano, 2001, p. 9).

[115] La cui regolamentazione è rintracciabile, per esclusione, nell'art. 391-*sexies* c.p.p. (in tal senso, v. N. TRIGGIANI, *Le investigazioni difensive*, Milano, 2002, p. 358).

Innanzitutto, la modalità di accesso cui si riferisce la disposizione codicistica ha carattere intrinsecamente "palese": il difensore, infatti, deve preventivamente ottenere l'accordo di colui che ha la disponibilità del luogo. Una modalità, quest'ultima, all'evidenza incompatibile con l'impiego di artifici e raggiri diretti a camuffare la propria identità.

S'immagina l'obiezione: nel caso che ci occupa, il consenso – ancorché viziato – è stato volontariamente manifestato dall'utente.

La censura, tuttavia, non sembra cogliere nel segno, quantomeno per un duplice ordine di ragioni.

In primo luogo, il secondo comma dell'art. 391-*septies* c.p.p. obbliga il difensore ad avvertire il destinatario dell'atto della facoltà di farsi assistere da un soggetto idoneo *ex* art. 120 c.p.p.; una chiara conferma, quest'ultima, del fatto che la disposizione sia stata pensata per essere applicata con esclusivo riferimento alle ipotesi in cui il patrocinante manifesti la propria identità e instauri una relazione diretta con il legittimo titolare del luogo al quale intende accedere. Del resto, lo stesso art. 14, comma 2, delle "Regole di comportamento del penalista nelle investigazioni difensive"[116] stabilisce che, quando intendono compiere un accesso a un luogo privato o non aperto al pubblico, i soggetti della difesa, nel richiedere l'anzidetta autorizzazione del disponente, «lo avvertono della propria qualità» e della natura dell'atto da compiere. È evidente, dunque, che l'attività di accesso ai luoghi, al pari di ogni altra operazione di indagine tipizzata agli artt. 391-*bis* ss. c.p.p., presuppone, sempre e comunque, la necessità che l'avvocato (o il suo delegato) si mostri "per quello che è".

In secondo luogo, si ricordi che la Corte di cassazione ha affermato a più riprese che l'atto tipizzato all'art. 391-*septies* c.p.p. compendia solamente la facoltà di ispezionare i luoghi *ivi* indicati, non anche quella di perquisirli al fine di acquisire eventuali documenti (come accade, invece, nel caso della *false friends tecnique*); un'operazione, quest'ultima, che, a detta dei giudici, è espressamente consentita solo con riguardo alla richiesta di documentazione alla pubblica amministrazione (art. 391-*quater* c.p.p.)[117].

Una volta esclusa la riconducibilità della "tecnica dei falsi amici" dal novero delle attività di indagine difensiva tipiche, occorre chiedersi se l'impiego di un profilo *fake* per accedere a informazioni ristrette possa comunque considerarsi legittimo. Per rispondere al quesito, in realtà, è necessario preliminarmente interrogarsi circa l'ammissibilità o meno nel modello processuale italiano di vere e proprie "indagini difensive innominate".

Nella vigenza dell'art. 38 disp. att. c.p.p., l'individuazione del contenuto dell'attività di investigazione difensiva era sostanzialmente lasciata alla prassi applicativa. La genericità della formulazione utilizzata e la mancanza di una qualsivoglia regolamentazione circa la tipologia di atti esperibili e la loro modalità di svolgimento (nonché di utilizzabilità), infatti, avevano indotto una parte della dottrina ad affermare che «tutto ciò che non [è] espressamente vietato è da considerarsi lecito»[118], per di più a fronte di un'attività

[116] "Regole di comportamento del penalista nelle investigazioni difensive", testo approvato il 14 luglio 2001 dal consiglio delle camere penali con le modifiche approvate il 19 gennaio 2007 e il 17 dicembre 2022, e modificato, da ultimo, il 4 febbraio 2023.

[117] Cass. pen., Sez. II, 12 ottobre 2005, Giambra.

[118] A. CRISTIANI, sub *Art. 38*, in *Commentario al nuovo codice di procedura penale. La normativa complementare*, coordinato da M. Chiavario, vol. I, Torino, 1989, p. 157.

procedimentale il cui fondamento era – ed è – rintracciabile nel diritto (inviolabile) di difesa tecnica. In pendenza della vecchia disciplina, pertanto, il sistema si basava su un principio di atipicità delle indagini difensive.

A seguito della novella del 2001 – che, come detto, ha cristallizzato le singole attività esperibili nel corso delle indagini difensive –, si è posto il problema di stabilire se questa "libertà delle forme" potesse considerarsi ancora valevole, specialmente a fronte del nuovo art. 327-*bis*, comma 1, c.p.p., ove si prevede che il patrocinante possa svolgere le investigazioni difensive «nelle forme e per le finalità stabilite nel titolo VI-*bis*» del libro V del codice di rito.

La risposta che deve offrirsi sembra essere positiva, specie facendo leva sulla necessaria applicazione del principio di parità delle armi nel contesto delle indagini preliminari: la possibilità conferita agli organi pubblici di svolgere attività atipiche – si è condivisibilmente affermato – dovrebbe essere garantita anche alla difesa[119]. È solo in tal modo, del resto, che potrebbe realizzarsi una piena equiparazione tra le parti, senza degradare in diritto alla prova (art. 24, comma 2, Cost.) «a mera eventualità, ossia […] ad una mera possibilità»[120].

Ciò nondimeno, sembra opportuno individuare con precisione i limiti entro cui dette operazioni atipiche possono essere svolte. Al pari delle attività innominate realizzate dalla polizia giudiziaria, infatti, non v'è dubbio che anche quelle riferibili al difensore debbano essere ricondotte entro confini ben definiti. In assenza di riferimenti normativi, sembra potersi affermare che qualunque indagine difensiva atipica incontri due limiti di carattere generale: l'atto deve ritenersi consentito purché rientri nel penalmente lecito[121] (*i*) e non incida sui diritti e le libertà fondamentali di terzi[122] (*ii*).

In queste coordinate teoriche, è possibile ritenere che l'inganno proprio delle operazioni di *false friends tecnique* influisca sulla legittimità delle stesse e, di riflesso, sull'utilizzabilità del materiale eventualmente acquisito.

In primo luogo, l'iscrizione a un *social network* mediante identità falsa, come già ricordato, integra di per sé gli estremi del delitto previsto e punito all'art. 494 c.p.

In secondo luogo, è ragionevole affermare che le indagini difensive trovino un limite invalicabile nella *privacy* dei terzi coinvolti dall'atto intrusivo (nel caso che ci occupa, il

---

[119] L. PARLATO, *Le nuove disposizioni in materia di indagini difensive. Commento alla legge 7 dicembre 2000, n. 397*, Torino, 2001, p. 54. In termini sostanzialmente non dissimili, v. N. TRIGGIANI, *Le investigazioni difensive*, cit., p. 221; e, nella manualistica, P. TONINI – C. CONTI, *Manuale di procedura penale*, Milano, 2023, p. 701, per i quali non può ritenersi «esclusa quella facoltà, insita nel diritto di difendersi provando, che consiste nel far svolgere investigazioni anche mediante atti atipici, come pedinamenti, registrazioni di colloqui in luoghi pubblici, conversazioni informali mediante telefono ecc.». Ricava la legittimità delle attività di investigazione atipiche dal disposto dell'art. 327-*bis* c.p.p., C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., p. 252.

[120] M. NOBILI, *Prove «a difesa» e investigazioni di parte nell'attuale assetto delle indagini preliminari*, in *Riv. it. dir. proc. pen.*, 1994, p. 413.

[121] Secondo N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, cit., p. 206, il diritto alla ricerca della prova in capo alla difesa dovrebbe «atteggiarsi non solo a diritto alla prova legittima, bensì a diritto alla prova lecita».

[122] P. TONINI – C. CONTI, *Manuale di procedura penale*, cit., p. 701. Come sottolinea C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., p. 252, «dal sistema pare ricavarsi che al difensore siano vietati gli atti lesivi di diritti fondamentali […] e che i dati probatori eventualmente acquisiti siano inutilizzabili ai sensi dell'art. 191. Questo divieto vale anche nel contesto della attività investigativa atipica».

target destinatario della richiesta di *follow*). In realtà, è ben vero che, in linea generale, deve ritenersi accolto dal sistema processuale un principio di prevalenza del diritto di difesa rispetto a quello alla riservatezza[123], nel senso che quest'ultimo è destinato a soccombere tutte le volte in cui il difensore abbia necessità di acquisire dati e informazioni aventi carattere personale e riservato, ancorché a seguito di un *placet* giurisdizionale (come nelle ipotesi di cui agli artt. 391-*quater*, comma 3 e 391-*speties*, comma 1, c.p.p.). Epperò, questo principio può trovare applicazione solo con riguardo allo svolgimento di attività investigative tipiche, rispetto alle quali il legislatore ha effettuato *ex ante* un giudizio di prevalenza del "diritto di difendersi investigando" rispetto al diritto alla riservatezza dei terzi. Per contro, con riguardo alle operazioni atipiche – al pari di quanto si è sostenuto in relazione alle indagini d'accusa – le istanze di garanzia dei diritti fondamentali debbono godere del più ampio margine di tutela. L'art. 8 CEDU, alla luce dell'interpretazione proposta nei capitoli e nei paragrafi precedenti, nonché avallata dalla giurisprudenza europea, può essere qualificato, dunque, alla stregua di uno di quei "limiti esterni" identificati dalla miglior dottrina in relazione allo svolgimento delle indagini difensive[124].

La conclusione, peraltro, non è destinata a mutare neppure qualora l'impiego di identità fittizie avvenga per mano di un investigatore privato autorizzato *ex* art. 222 disp. att. c.p.p. Anche laddove si ritenga che questi possa «"camuffarsi" al fine di individuare fonti di prova altrimenti non reperibili», potendo ricorrere «a quello che è stato definito "l'inganno buono"»[125], non sembra comunque possibile spingersi tanto in là da consentire l'impiego di tecniche penalmente illecite e lesive dei diritti fondamentali.

Superfluo appare, infine, sottolineare come l'esclusione della *false friends tecnique* dal novero delle attività di investigazione difensiva non ponga alcun problema sul versante della garanzia sancita all'art. 111, comma 2, Cost. È noto – e la Corte costituzionale lo ha sottolineato a più riprese[126] – che il principio di parità delle armi tra accusa e difesa non comporti necessariamente un'identità tra i poteri processuali del pubblico ministero e quelli attribuiti alla difesa, né, tantomeno, un'identità di mezzi e strumenti investigativi[127]. Anche qualora, come si è auspicato, il legislatore intervenisse per approntare una disciplina *ad hoc* che consenta al pubblico ministero di impiegare detto strumento per fini investigativi, non parrebbe comunque sussistere un «generale squilibrio a danno di una parte»[128], presupposto necessario per avanzare dubbi di legittimità costituzionale della normativa.

---

[123] Sul punto, v., da ultimo, M. TORRE, Privacy *e indagini penali*, Milano, 2020, p. 143.

[124] P. TONINI, *L'investigazione difensiva e la legge sulla* privacy, in L. Filippi (a cura di), *Processo penale: il nuovo ruolo del difensore*, Padova, 2001, p. 517.

[125] Per le due ultime citazioni, v. P. TONINI – C. CONTI, *Manuale di procedura penale*, cit., p. 701.

[126] Cfr., ad es., Corte cost., 24 gennaio 2007, n. 26.

[127] In dottrina, v. M. CHIAVARIO, *Processo e garanzie della persona*, vol. II, Milano, 1984, p. 24; P. FERRUA, *Il "giusto processo"*, Torino, 2007, p. 49; E. MARZADURI, *La parità delle parti nel processo penale*, in *Quad. cost.*, 2007, p. 378.

[128] Nuovamente, M. CHIAVARIO, *Processo e garanzie della persona*, cit., p. 24.

CAPITOLO V

CAPTAZIONE E APPRENSIONE DELLE "INFORMAZIONI SEGRETE" CONTENUTE NELLE PIATTAFORME DIGITALI

SOMMARIO: 1. Le diverse modalità di accesso ai "dati riservati". – 2. Il sequestro probatorio del materiale presente in un profilo *social*. – 3. Il sequestro probatorio realizzato in ambiente *Cloud computing*: uno scenario ancora "nebuloso". – 4. *Nemo tenetur se detegere* e apprensione dei codici di accesso. – 4.1 *Touch ID* e *Face ID*: linee evolutive del diritto al silenzio nell'era della biometria. – 4.2 La valutazione *contra se* del contegno non collaborativo dell'imputato: la negazione giurisprudenziale del "diritto di esercitare i diritti". – 4.3 L'estensione del *social network privilege* alla persona non sottoposta a indagini. – 5. Accesso occulto e da remoto a informazioni non comunicative mediante *trojan horse*. – 6. L'acquisizione delle comunicazioni scritte e orali scambiate mediante le piattaforme di messaggistica istantanea. – 7. Tutela dei minori e cybersorveglianza delle *chat* di *instant messaging*: derive orwelliane della "Piccola Europa". – 8. Il ruolo dei *Social network provider* nell'apprensione delle informazioni segrete: verso un'esternalizzazione consapevole (e necessaria) della funzione perquirente

1. Le diverse modalità di accesso ai "dati riservati"

Proseguendo l'analisi nel solco della classificazione proposta in apertura[1], occorre adesso soffermarsi sull'impiego di tecniche investigative in grado di acquisire dati e informazioni aventi carattere segreto e riservato, rispetto alle quali vi è una totale assenza di pubblicità, intesa come astratta conoscibilità in capo a una platea indeterminata e indefinita di soggetti.

Trattasi, come può ben intuirsi, di una categoria alquanto eterogenea che può racchiudere in sé contenuti *social* aventi o meno carattere *stricto sensu* comunicativo. Si pensi, sul primo fronte, ai messaggi scambiati nella *chat* di *Whatsapp*, ai commenti privati alle *stories* pubblicate su *Instagram* o, ancora, alle *emoticon* inviate tramite *Messanger*. Nella seconda categoria, invece, possono essere annoverati tutti quei *bit* digitali presenti in un "profilo chiuso" che l'utente intende condividere solo con sé stesso, quali, ad esempio, i dati di contatto, l'*e-mail*, la data di nascita, la lista degli amici o, ancora, le persone e le pagine *web* "seguite".

In una prospettiva ancora germinale, e al fine di evitare possibili equivoci interpretativi, è opportuno sottolineare fin da subito come la divulgazione di tali informazioni al gestore della piattaforma (il *Social network provider*) – operazione svolta in maniera automatica e indipendente dalla volontà dell'utente – non incida in alcun modo sulla loro natura, per l'appunto, riservata; e, ciò, indipendentemente dal fatto che si tratti di informazioni aventi o meno carattere comunicativo. Invero, tanto nel caso in cui esse siano visibili solamente all'utente, quanto nell'ipotesi di comunicazioni realizzate mediante l'impiego di una *chat online*, la circostanza che il soggetto le abbia volontariamente trasferite al *provider* non può in alcun modo giustificare una *deminutio* delle garanzie poste a tutela dei diritti fondamentali di volta in volta in rilievo (*privacy*, segretezza, domicilio informatico, proprietà privata, etc.).

[1] Cfr. Parte II, Cap. II, par. 1.

A tal proposito, infatti, si è già avuto modo di ricordare come un eventuale richiamo alla dottrina americana della "terza parte" risulti all'evidenza inconferente: nella moderna era digitale, il SNP è chiamato a svolgere un ruolo meramente passivo, limitandosi a mettere a disposizione uno strumento di comunicazione e relazione sociale.

Ciò nondimeno, la distinzione tra atti comunicativi e non comunicativi, come si avrà modo di osservare, assume una portata dirimente, giacché incide direttamente sulla sfera di operatività dell'art. 15 Cost., volto a tutelare, precisamente, ogni forma di «corrispondenza» e di «comunicazione». Diviene, così, di esiziale importanza individuare il discrimine tra le due condotte, al fine di stabilire se, come e quando un provvedimento dell'«autorità giudiziaria» possa limitare quel diritto alla segretezza proclamato in termini di inviolabilità.

Ciò chiarito, le *social network private information* possono essere acquisite – volendo ricorrere a una classificazione inevitabilmente approssimativa – mediante il ricorso a due differenti modalità di apprensione. Innanzitutto, l'autorità giudiziaria potrebbe procedere attraverso un "accesso palese", ad esempio facendo ricorso al mezzo di ricerca della prova previsto agli artt. 253 ss. c.p.p. In alternativa, il pubblico ministero o la polizia giudiziaria – anche alla luce delle numerose difficoltà pratiche cui va incontro la predetta opzione investigativa, delle quali si dirà a breve – potrebbero ricorrere all'impiego dello strumento captativo, anche mediante *virus trojan*, in grado di acquisire, in tempo reale, i dati segreti contenuti nelle piattaforme.

Nei paragrafi che seguono, si procederà a esaminare distintamente entrambe le ipotesi.

Una precisazione, però, appare fin da ora necessaria. Il sequestro di un *computer* o di un *device* mobile, al pari dell'impiego del *trojan* di Stato, consente alla polizia giudiziaria di apprendere non solo le informazioni private contenute nelle piattaforme, ma anche ogni altro dato digitale presente nel terminale, pur se processualmente irrilevante. La dottrina più autorevole, del resto, ha messo in luce, da tempo, come una delle caratteristiche principali dell'investigazione digitale e della prova informatica debba rintracciarsi proprio nella «promiscuità» dei dati captati[2]. L'efficace locuzione allude al fatto che le informazioni digitali allocate tanto negli "spazi fisici" (come, ad esempio, lo *smartphone*), quanto nei "contenitori virtuali" (come nel caso del *cloud*), inglobano sia elementi di prova processualmente significativi, sia materiale «supersensibile»[3], del tutto estraneo al terreno delle indagini[4].

Da quanto detto, si ricava la necessità di compiere una duplice operazione esegetica.

---

[2] M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 287.

[3] G. DI CHIARA, *Atipicità e sistemi probatori: linee per una fenomenologia generale*, in V. Militello – A. Spena (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Torino, 2018, p. 385.

[4] È la stessa giurisprudenza di legittimità ad aver recentemente riconosciuto che «la natura eterogenea dei dati contenuti in un sistema informatico comporta l'eventualità che nel corso delle indagini informatiche vengano acquisite anche informazioni "sensibili" o "supersensibili", relative cioè alla sfera privata e intima dell'indagato» (Cass. pen., Sez. VI, 22 settembre 2020, n. 34265, in *Sist. pen.*, 14 gennaio 2021, con scheda di M. PITTIRUTI, *Dalla Corte di cassazione un* vademecum *sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali* omnibus). Per tale ragione, non v'è da stupirsi se la Corte europea dei diritti dell'uomo ha più volte affermato che il sequestro di uno *smartphone* eseguito da un'autorità pubblica comporta un'ingerenza nel diritto al rispetto della corrispondenza e, più in generale, della vita privata, così per come tutelati all'art. 8 CEDU (Corte edu, 17 dicembre 2020, *Saber c. Norvegia*).

Per un verso, occorre individuare se e quali diritti fondamentali vengono in gioco allorquando si tratta di acquisire questa tipologia di dati. Per altro verso, è opportuno muoversi alla ricerca di strumenti tecnico-giuridici in grado di limitare l'acquisizione ai soli dati processualmente rilevanti, escludendo dal compendio probatorio tutto quanto non sia strettamente necessario per l'accertamento dei fatti: del resto, «se è legittimo ricercare le tracce della illiceità, più discutibile è conoscere e soprattutto diffondere ciò che vi è estraneo»[5].

2. Il sequestro probatorio del materiale presente in un profilo *social*

Si muova dal dettato normativo. L'art. 253 c.p.p. disciplina un peculiare mezzo di ricerca della prova, il sequestro probatorio, finalizzato ad assicurare al procedimento penale una cosa mobile o immobile necessaria per l'accertamento dei fatti. L'acquisizione avviene mediante lo spossessamento coattivo della *res* e la contestuale imposizione di un vincolo di indisponibilità sulla medesima. Oggetto del sequestro, come noto, sono esclusivamente il corpo del reato o le cose a esso pertinenti.

L'avvento della prova tecnologica, tuttavia, ha messo in crisi questo lineare marchingegno investigativo. Agli inizi degli anni '90 dello scorso secolo, infatti, dottrina e giurisprudenza dubitavano della possibilità di ricondurre i dati digitali (*rectius*, i *bit*) nel concetto di "cose" sequestrabili, giacché queste erano interpretate in senso "fisico-analogico", escludendo così la possibilità di ricondurvi ciò che, per sua natura, è, invece, immateriale[6].

L'approvazione nel 2008 della legge di recepimento della Convenzione di Budapest sul *Cybercrime*, però, ha, almeno in parte, scardinato questo *modus pensandi*. Oggigiorno, infatti, nessuno può fondatamente dubitare del fatto che le informazioni digitali devono essere qualificate come "cose" e, dunque, possano essere oggetto di sequestro. L'assunto si fonda sulla distinzione che, in ambito informatico-giuridico, intercorre tra il "contenitore", cioè il dispositivo elettronico (*smartphone*, *computer*, *tablet*, etc.) e il "contenuto", ovverosia i dati digitali *ivi* conservati[7]. Nella realtà *hi-tech*, infatti, le informazioni elettroniche vivono di vita propria, posto che esse esistono indipendentemente dal supporto fisico nel quale sono immagazzinate (si legga, incorporate). È per tale motivo, d'altro canto, che questo tipo di informazione e, più in generale, il documento informatico, in quanto scindibile dal supporto che lo contiene, può essere agevolmente trasferito su altri *devices* e condiviso con terzi. Al contempo, però, questa caratteristica genera problemi in punto di modificabilità e alterabilità del dato, in quanto il passaggio da un supporto a un altro potrebbe provocarne un'alterazione, pure involontaria.

---

[5] G. SPANGHER, *Ragionamenti sul processo penale*, Milano, 2018, p. 114.

[6] A. MONTI, *La nuova disciplina del sequestro informatico*, in L. Lupária (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 202.

[7] L'intuizione si deve, come noto, a P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 401 ss., il quale, per primo, ha proposto di distinguere tra documento tradizionale e documento informatico alla luce del metodo di incorporazione del dato che è, rispettivamente, materiale (nel senso che la rappresentazione non esiste senza la presenza del supporto fisico) e immateriale (nel senso che la rappresentazione è indifferente rispetto alla scelta del tipo di supporto fisico nel quale l'informazione è incorporata).

In questo contesto, si innestano le novità apportate dalla richiamata l. 48/2008, il cui scopo dichiarato era quello di predisporre strumenti in grado di tutelare la genuinità del dato informatico, a fronte della presa d'atto di una vulnerabilità congenita della prova digitale. Pur non delineando, in maniera chiara, precisa e dettagliata, le *best practices* da seguire al momento dell'analisi informatica (*digital forensics*)[8], il legislatore ha sottolineato come tali procedure debbano garantire «la conservazione dei dati originali e […] impedirne l'alterazione» (art. 247, comma 1-*bis* c.p.p.), ovverosia assicurare la «conformità dei dati acquisiti a quelli originali e la loro immodificabilità» (art. 254-*bis* c.p.p.)[9].

Ebbene, proprio il *discrimen* tra "dato digitale" e "supporto fisico" assume una certa consistenza anche con riguardo all'apprensione delle informazioni segrete contenute nei *social network*. Generalmente, infatti, l'accesso alla propria pagina personale o alla *chat* avviene tramite applicazioni installate sullo *smartphone* o su altri dispositivi elettronici di uso quotidiano. Questi ultimi, alla luce della proposta distinzione, rappresentano i "contenitori" o, meglio, la base materiale nella quale sono incorporati i dati digitali ("contenuto"), composti da una sequenza di *bit*.

A tal proposito, una delle principali questioni che ha catalizzato l'attenzione di dottrina e giurisprudenza è rappresentata dalla corretta individuazione dell'oggetto e dell'estensione del sequestro di dati informatici, come quelli rinvenibili nelle piattaforme di *sharing*.

Sul primo versante, occorre stabilire se l'autorità inquirente possa procedere con l'asportazione del supporto che contiene i dati digitali ovvero se debba limitarsi all'apprensione dei singoli *file* informatici. L'alternativa non è di poco momento: il sequestro dell'intero *device*, oltre a incidere su beni di rilievo costituzionale[10], parrebbe lesivo del principio di pertinenzialità che governa l'attività probatoria, giacché, in tal modo, l'autorità inquirente finisce per apprendere una serie di dati processualmente irrilevanti rispetto al contenuto dell'addebito provvisorio.

L'interrogativo sul quale ci si interroga, a ben vedere, trae origine da una disposizione pattizia, il cui contenuto appare tutt'altro che lineare. L'art. 19 della Convenzione di Budapest prevede la possibilità per le autorità competenti di perquisire, sequestrare o «accedere in modo simile» a un «sistema informatico o parte di esso e ai dati informatici *ivi* immagazzinati», nonché a «un supporto per la conservazione di dati informatici nel quale i dati stessi possono essere immagazzinati». Come esplicitato nel *report* illustrativo redatto dal Comitato dei ministri del Consiglio d'Europa, il termine «sequestrare» assume,

[8] La scelta appare condivisibile. Come è stato osservato, infatti, l'individuazione a livello legislativo di una singola tecnica di acquisizione si pone in contrasto con l'idea di una scienza informatica "in continua evoluzione", non potendosi individuare, allo stato dell'arte, una modalità apprensiva in grado di imporsi sulle altre. Senza voler considerare, in aggiunta, come la scelta di una metodologia piuttosto che l'altra dipenda, nella maggior parte dei casi, dalle circostanze del caso concreto (M. DANIELE, *La prova digitale nel processo penale*, cit., p. 293). Concordi, tra i molti, L. LUPÁRIA, *La ratifica della convenzione* cybercrime *del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.*, 2008, p. 719; L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4517; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 136.

[9] Riferimenti simili in merito alla necessità di garantire la non alterabilità del dato informatico si rinvengono pure agli artt. 259, comma 2, 352, comma 1-*bis* e 354, comma 2.

[10] Tra questi, ad esempio, possono annoverarsi la riservatezza, la libertà di iniziativa economica e la libertà di comunicazione.

nell'ambito della Convenzione, un duplice significato: a) prendere («*to take away*») il mezzo fisico sul quale i dati o le informazioni sono registrati; b) oppure, fare e trattenere una copia di detti contenuti[11]. La normativa sovranazionale, dunque, considera legittimamente sequestrabili tanto il dispositivo fisico, quanto le informazioni *ivi* incorporate.

L'assunto, come noto, è stato accolto dalla giurisprudenza di legittimità italiana, la quale ha espressamente riconosciuto piena autonomia ai dati informatici rispetto al loro contenitore materiale[12]. Il Supremo consesso, nella sua più autorevole composizione, ha difatti ritenuto opportuno distinguere il «contenitore rispetto al contenuto», di talché «l'oggetto di un […] provvedimento di sequestro può riguardare, sussistendone la necessità, l'intero sistema (come nel caso in cui l'apprensione sia necessaria per esaminare grosse quantità di dati) […], ovvero il singolo dato, che ha certamente una sua identità fisica, essendo modificabile e misurabile»[13].

La conclusione, senz'altro condivisibile, è stata coltivata nei successi arresti pretori che, sul punto, hanno recentemente fornito un vero e proprio *vademecum* in tema di acquisizioni probatorie informatiche[14].

Nella prassi, il pubblico ministero suole disporre, con decreto motivato, una perquisizione locale (*i*) finalizzata all'apprensione del *device* (ad esempio, uno *smartphone*); una volta individuato, la polizia giudiziaria, posto che l'estrazione dei *bit* seduta stante mediante il ricorso alla cd. *live analisys* risulta perlopiù impraticabile, specialmente per ragioni tecniche che incidono direttamente sulla genuinità del dato[15], procede con il sequestro del terminale (si legga, cosa pertinente al reato[16]), al fine di acquisire i dati *ivi* contenuti (*ii*). A questo

---

[11] COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Explanatory Report to the Convention on Cybercrime*, 23 novembre 2001, punto n. 197.

[12] Cass. pen., Sez. VI, 24 febbraio 2015, Rizzo.

[13] Cass. pen., Sez. Un., 20 luglio 2017, n. 40963. Per un approfondito commento alla pronuncia, v. L. BARTOLI, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. pen.* web., 5 marzo 2018.

[14] Il riferimento è a Cass. pen., Sez. V, 22 settembre 2020, n. 34265, cit. La sentenza si fa apprezzare anche da un punto di vista di teoria generale della prova, giacché riconosce apertamente che «l'impatto della c.d. prova digitale sul processo penale ha imposto una rimeditazione dei modelli concettuali e dell'approccio investigativo tradizionale, proprio in ragione della particolare natura del dato informatico» (par. 4).

[15] Non si disconoscono, invero, i vantaggi propri del cd. esame *in loco*: esso consente alla polizia giudiziaria di apprendere dati utili per l'immediata prosecuzione delle indagini ed evita i rischi connessi alla fase di trasporto del *device* in laboratorio; un'operazione, quest'ultima, che richiede una serie di accortezze particolari, quali, ad esempio, l'isolamento del dispositivo, l'imballaggio e la conservazione in luoghi idonei. Ciò nondimeno, vi sono, per contro, numerose controindicazioni: la *live analisys* rischia di compromettere i dati contenuti nel dispositivo, specialmente se eseguita in determinanti contesti nei quali vi è una criminalità ad alta specializzazione tecnologica; l'autorità giudiziaria non è perlopiù in grado di sapere *ex ante* che cosa ricercare all'interno del *device* e non è supportata, nella maggior parte dei casi, da personale formato *ad hoc*. Per tali ragioni, devono condividersi le conclusioni degli esperti più accreditati, ove si sottolinea una preferenza per una *remote analisys* a discapito di una *live forensics* (cfr. V.G. CALABRÒ, *Mobile device and mobile cloud computing forensics*, Torino, 2016, *passim*).

[16] Non può dubitarsi della riconducibilità dello *smartphone* o del *computer* in tale categoria. Poiché il legislatore dell'88 non ha definito normativamente il concetto di "cose pertinenti al reato", affidando questo compito all'interpretazione giurisprudenziale, i giudici di legittimità hanno adottato una nozione particolarmente estesa. Si parla, in proposito, di tutti quegli elementi «che sono in rapporto indiretto con la fattispecie criminosa concreta e risultano strumentali all'accertamento dei fatti, ovvero quell[i] necessari alla dimostrazione del reato e delle sue modalità di preparazione ed esecuzione, alla conservazione delle tracce, all'identificazione del colpevole, all'accertamento del movente ed alla determinazione dell'*ante factum* e del *post factum* comunque ricollegabili al reato, pur se esterni all'*iter criminis*, purché funzionali all'accertamento

punto, l'esperto informatico dovrà realizzare, in laboratorio, una copia-mezzo (cd. copia servente); egli, in breve, è chiamato a estrapolare, mediante la tecnica del *bit stream imagine*[17], un clone dell'originale che viene reso immodificabile mediante la creazione di un'impronta digitale – tecnica di *hashing* – atta a garantire l'integrità del dato, cd. copia forense o copia *bit* a *bit* (*iii*)[18]. Dopo aver restituito il *device* al legittimo titolare[19], l'autorità procedente deve verificare quali, tra i dati presenti nella cd. copia originale, sono legali da un vincolo di pertinenzialità rispetto al reato contestato, mediante la realizzazione di una vera e propria perquisizione informatica (*iv*).

L'*iter* appena descritto rappresenta, a tutti gli effetti, un'attività di indagine complessa, composta da una serie di operazioni concatenate tra loro che incarnano, come si è cercato di evidenziare, ben quattro differenti mezzi di ricerca della prova.

Con riguardo alla prima fase (*i*), viene da chiedersi se l'apprensione del *device* (fisso o mobile) possa ancora essere qualificata alla stregua di una perquisizione locale. In proposito, si è già ricordato come i dispositivi elettronici di uso quotidiano rappresentino vere e proprie

---

del fatto ed all'individuazione dell'autore» (Cass., sez. IV, 17 novembre 2010, n. 2622. Conforme, da ultimo, Cass. pen., Sez. VI, 13 marzo 2019, n. 37639).

[17] Ovverosia l'esatto duplicato di ogni *bit* che compone il disco rigido. Trattasi, perciò, di una procedura che consente di riprodurre il contenuto del dispositivo in tutte le sue caratteristiche, «con la stessa disposizione dei *file*, i pezzi di *file*, i *file* danneggiati, i frammenti di *file*» (così, G. ZICCARDI, *La procedura di analisi della fonte di prova digitale*, in L. Lupária – G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 64).

[18] Va rammentato, però, che la modalità copia *bit* a *bit* non è usata oggi con riguardo ai *device* mobili, come, ad esempio, gli *smartphone*, a causa di limiti tecnico-informatici legati perlopiù alla cifratura del sistema. È preferibile, perciò, impiegare altre tecniche come il *backup*, il *file system* o, *in extremis*, l'esecuzione di una semplice fotografia di quanto rilevato (sul punto, v. M. FERRAZZANO – L. SUMMA, *La selezione dei dati informatici in ambito giudiziario: prassi e modalità applicative*, in R. Brighi (a cura di), *Nuove questioni di informatica forense*, Roma, 2022, p. 75).

In dottrina, peraltro, non vi è unanimità di pensiero in merito alla qualificazione giuridico-processuale di questa attività (*rectius*, esecuzione della copia-mezzo). La duplicazione del dato informatico è stata ricondotta da una parte dei commentatori nell'alveo del sequestro probatorio, giacché essa si tradurrebbe «nell'ablazione di una *res*, sia pure immateriale» (per questa opinione, v., ad es., M. PITTIRUTI, Digital evidence *e procedimento penale*, Torino, 2017, p. 38). L'assunto, peraltro, viene giustificato anche alla luce del fatto che a seguito dell'ablazione l'interessato rimane sì nella disponibilità del proprio *device*, ma perde il diritto a essere l'utilizzatore esclusivo dei *file* in esso contenuti (in tal senso, O.S. KERR, *Searches and Seizures in a Digital World*, in *Harvard Law Review*, 2005, p. 558). Altri Autori, invece, dubitando di tale ricostruzione, hanno sottolineato che «mentre il sequestro è un atto di coercizione reale che crea un vincolo di indisponibilità sulla *res* e ne determina lo spossessamento, la creazione di una copia non determina invece simili conseguenze. Quest'ultima permette soltanto la duplicazione dei dati, mentre quelli originali restano nel possesso del soggetto» (così, S. SIGNORATO, *Le indagini digitali*, cit., p. 226-228). Infine, una terza corrente di pensiero suggerisce di ricondurre tali operazioni nella disciplina delle perquisizioni informatiche *ex* art. 247, comma 1-*bis* c.p.p., giacché il riferimento alle «misure tecniche idonee» contenuto della disposizione sarebbe in grado di inglobare in sé tanto l'attività di ricerca in senso stretto che quella di copiatura (P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, cit., p. 1605).

[19] Sulla necessità di un'immediata restituzione all'avente diritto a seguito dell'estrazione della copia-clone, v. Cass. pen., Sez. VI, 22 settembre 2020, n. 34265, cit., per la quale «l'autorità giudiziaria, al fine di esaminare un'ampia massa di dati i cui contenuti sono in astratto – potenzialmente – rilevanti per le indagini, può disporre un sequestro dai contenuti molto estesi, provvedendo, tuttavia, nel rispetto del principio di proporzionalità ed adeguatezza, alla immediata restituzione delle cose sottoposte a vincolo non appena sia decorso il tempo ragionevolmente necessario per gli accertamenti e, in caso di mancata tempestiva restituzione, l'interessato può presentare la relativa istanza e far valere le proprie ragioni, se necessario, anche mediante i rimedi impugnatori offerti dal sistema».

«protesti tecnologic[he] della persona»[20], nonché "oggetti sociali di comunicazione", cioè strumenti che consentono all'individuo di interagire con il prossimo mediante l'uso dei *social network*[21]. Per tale ragione, sarebbe forse opportuno che queste parti "esterne" del corpo umano fossero oggigiorno quantomeno equiparate a quei beni che «abitualmente sono portati sulla persona (come portafogli, portamonete ecc.) o ad immediato contatto di essa (come borse, bordelli e borsette)»[22], rispetto ai quali la Corte costituzionale ha riconosciuto la piena operatività delle tutele previste all'art. 13 Cost. Di conseguenza, non sembra azzardato ritenere che un'eventuale loro apprensione debba essere ricondotta, più propriamente, nell'ambito di una perquisizione personale.

Più complesse sono, invece, le considerazioni che debbono svolgersi con riguardo al sequestro probatorio del dispositivo elettronico (*ii*).

A seguito delle Sezioni Unite Andreucci[23], la giurisprudenza di legittimità pare essersi assestata su un'interpretazione volta a garantire una maggior tutela del principio di proporzionalità (tra il contenuto del provvedimento ablativo e le esigenze di accertamento dei fatti oggetto delle indagini), la cui applicazione nell'ambito del sequestro probatorio appare ormai unanimemente riconosciuta[24]. A tal proposito, si ritiene che lo spossessamento materiale (*rectius*, il sequestro) di un *computer* o di uno *smartphone*, in luogo

---

[20] G. DI CHIARA, *Atipicità e sistemi probatori: linee per una fenomenologia generale*, cit., p. 385. Come sottolinea M. GIALUZ, *Premessa*, in Id. (a cura di), *Le nuove intercettazioni. Legge 28 febbraio 2020 n. 7*, in *Dir. Internet*, 2020, Suppl. al n. 3, p. 7, nei «dispositivi tecnologici di uso comune – e, in particolare, in quello "strumento degli strumenti" che, per i filosofi antichi era la mano e per i contemporanei è lo *smartphone* – c'è l'intera nostra vita e […] essi rappresentano una vera estensione della nostra mente». Nello stesso senso, v., esplicitamente, S. SIGNORATO, *Le indagini digitali*, cit., p. 70.

[21] Con plastica efficacia, L. LUPÁRIA, Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, diretto da G. Spangher, in G. Garuti (a cura di), *Modelli differenziati di accertamento*, t. I, Torino, 2011, p. 374, sottolinea come «il *computer* è divenuto, nelle sue varie declinazioni, il centro motore per la gestione dei propri interessi, il principale contenitore dei frammenti di vita e dei dati sensibili di ciascuno, la memoria sempre più estesa di attività e addirittura di spostamenti fisici, oltre che un veicolo essenziale per la comunicazione».

[22] Corte cost., 31 marzo 1987, n. 88. A tal proposito, come osserva A. CAMON, *Cavalli di troia in Cassazione*, in *Arch. n. proc. pen.*, 2017, p. 95, «se la necessità di rispettare la riserva di legge e quella di giurisdizione vale quando l'autorità intende frugare in un portafoglio, sarebbe grottesco non valesse per uno *smartphone*; chiunque capisce che nel secondo caso la lesione all'intimità è incomparabilmente superiore: il cellulare è ormai compagno di viaggi, diario, agenda, memoria, scrigno d'informazioni».

[23] Cass. pen., Sez. Un., 20 settembre 2017, n. 40963, cit.

[24] Il canone di proporzionalità, come risaputo, è espressamene previsto nel codice di rito solamente con riguardo ai criteri di scelta delle misure cautelari *de libertate* (art. 275 c.p.p.), ma la giurisprudenza lo ha condivisibilmente esteso anche al settore delle misure cautelari reali, onde evitare un'indebita compressione del diritto di proprietà e di libera iniziativa economica privata (cfr., da ultimo, Cass. pen., Sez. V, 14 marzo 2017, n. 16622). Se un tanto è vero, non v'è ragione per inibirne l'operatività in relazione a qualunque atto investigativo che imprima un vincolo di indisponibilità su una *res*, posto che la necessità di limitare al minimo il diritto in gioco viene in rilievo non solo nelle misure cautelari, ma anche nel sequestro probatorio (così, Cass. pen., Sez. Un., 20 settembre 2017, n. 40963, cit.). Per di più, la stessa giurisprudenza di legittimità ha osservato come l'applicazione del principio di proporzionalità in materia di sequestri «non solo risponde ad un'esigenza immanente al sistema processuale penale ed a criteri generali di ragionevolezza, ma trova riscontro specifico nella disposizione di cui all'art. 258 c.p.p., comma 4, che – nel prevedere il sequestro di documenti che fanno "parte di un volume o di un registro" – esclude che, di norma, possa procedersi a sequestri di masse indistinte di documenti senza una specifica ragione. È dunque illegittimo, per violazione del principio di proporzionalità e adeguatezza, il sequestro a fini probatori di un sistema informatico – quale è un *personal computer* – che conduca, in difetto di specifiche ragioni, ad una indiscriminata apprensione di tutte le informazioni *ivi* contenute» (Cass. pen., Sez. VI, 14 novembre 2018, n. 4857).

dell'estrapolazione con copia forense di singoli dati, debba ritenersi legittimo solo a condizione che: a) il decreto autorizzativo indichi le specifiche ragioni che impongono un'apprensione massiva; b) l'autorità procedente provveda alla immediata restituzione delle cose non appena sia decorso il tempo ragionevolmente necessario per lo svolgimento degli accertamenti[25]. L'imposizione di una sorta di "motivazione rafforzata" in capo al pubblico ministero che voglia disporre un sequestro *omnibus* consente – nella prospettiva adottata dal Supremo consesso (che merita di essere condivisa) – di evitare che tale strumento assuma una valenza meramente esplorativa rispetto a notizie di reato diverse e ulteriori da quella per cui il sequestro è stato disposto[26], nonché a garantire un'effettiva giustiziabilità del provvedimento ablativo.

Ciò nondimeno, le considerazioni svolte in merito alla pervasività del sequestro di dati informatici – mezzo di ricerca della prova che consente oggigiorno di acquisire molte più informazioni rispetto a una "semplice" perquisizione domiciliare, giacché in grado di eseguire una vera e propria "radiografia digitale" della persona[27] – inducono a prospettare la necessità di un intervento novellistico volto a introdurre una regolamentazione *ad hoc*. La miglior dottrina, del resto, non ha mancato di sottolineare le differenze qualitative e quantitative del "sequestro digitale" rispetto al corrispettivo analogico, nonché il maggior grado di intrusività del primo nella sfera di riservatezza del bersaglio[28]. Se è vero che alla nozione di "corpo umano" può essere riconosciuta una triplice dimensione, ovverosia quella fisica, psichica e digitale[29], un corretto inquadramento del tema *de quo* presuppone un'opera di delimitazione dei confini proprio di quella dimensione *lato sensu* informatica.

A tal fine, non sembra potersi dubitare della riconducibilità dei moderni dispositivi di comunicazione e relazione sociale nell'ambito del concetto di "domicilio informatico"[30]: lo *smartphone*, quale proiezione nell'etere dell'essere umano, rappresenta l'oggetto di quel «diritto di casa [2.0]»[31] volto a tutelare le attività svolte quotidianamente e stabilmente da ogni persona. Se il domicilio analogico è, secondo una nota definizione, «la proiezione

---

[25] Cfr. Cass. pen., Sez. V, 23 marzo 2022, n. 15648, ove si sottolinea che «le perquisizioni ed il sequestro informatico sono illegittimi se volti ad ottenere l'acquisizione indiscriminata dei dati contenuti nei supporti informatici da sottoporre a sequestro, senza alcun criterio selettivo degli stessi e senza l'indicazione del collegamento tra il reato contestato e i dati informatici che si intendono vincolare»; Cass. pen., Sez. II, 23 febbraio 2023, n. 17604.

[26] Sull'illegittimità del sequestro *ad explorandum*, Cass. pen., Sez. VI, 15 settembre 2020, n. 30225.

[27] «Uno *smartphone* non è un telefonino, è un pezzo di casa che ci si porta appresso, ci sono più cose lì dentro che nelle nostre abitazioni»: così, F. CAPRIOLI, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, in L. Lupária – L. Marafioti – G. Paolozzi (a cura di), *Dimensione tecnologica e prova penale*, Torino, 2019, p. 50.

[28] V., per tutti, le riflessioni offerte da G. LASAGNI, *Tackling Phone Searches in Italy and the United States: Proposals for a Technological Rethinking of Procedural Rights and Freedoms*, in *New Journal of European Criminal Law*, 2018, p. 394, la quale mette in luce come «*the requirements necessary to consider proportionate, and therefore legitimate, the search of digital data in a democratic society may differ from those applicable to other physical objects, in light of the "qualitative" and "quantitative" differences typical of digital devices highlighted above, and especially, of the greater degree of privacy intrusion characterized by digital searches*».

[29] In questi termini, richiamando la nota classificazione proposta da Stefano Rodotà, v., nuovamente, G. LASAGNI, *Tackling Phone Searches in Italy and the United States*, cit., p. 394.

[30] Cfr., *amplius*, Parte II, Cap. I.

[31] M. PISANI, *La tutela penale della «riservatezza»: aspetti processuali*, in *Riv. it. dir. proc. pen.*, 1967, p. 788.

spaziale dell'essere umano»[32], lo *smartphone* e i *social network* possono essere senz'altro raffigurati come la proiezione digitale dell'*homo tecnhologicus*[33]. Per tale ragione, un'interpretazione evolutiva e in *bonam partem* dell'art. 14 Cost. impone, *de lege lata*, di estendere le garanzie *ivi* previste anche all'ipotesi del sequestro informatico. Ne deriva, sul versante processuale, la necessità che eventuali limitazioni siano realizzate nel rispetto delle «garanzie prescritte per la tutela della libertà personale» (art. 14, comma 2, Cost.), esigendosi, in particolare, un «atto motivato dell'autorità giudiziaria» (art. 13, comma 1, Cost.).

Degno di nota, a tal proposito, è il recente Disegno di legge n. 806/2023 recante "Modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, *smartphone* e memorie digitali"[34], con il quale i senatori promotori – nel prospettare l'introduzione di un nuovo art. 254-*ter* c.p.p. – hanno colto appieno la necessità di circondare questo mezzo di ricerca della prova da nuove e più efficaci garanzie[35].

La proposta non può che essere salutata con favore.

L'aspetto più delicato, sul quale debbono essere espresse alcune riserve, riguarda, però, la mancata previsione in capo all'organo giurisdizionale (e non giudiziario) del potere di disporre il sequestro[36]. Una volta riconosciuta la vorace pervasività di questo mezzo di indagine, se ne dovrebbe dedurre – al pari di quanto previsto in materia di tabulati telefonici[37] – l'indispensabilità di un vaglio giurisdizionale[38], sottraendo all'organo d'accusa il potere di disporre quello che oggi può senz'altro essere definito come l'atto di indagine (palese) più pervasivo che esista. Di questa esigenza, occorre prenderne atto, si è fatto carico il dibattito parlamentare: in forza di un emendamento presentato in data 15 febbraio 2024, la Commissione giustizia del Senato ha modificato il testo originario del Disegno di legge – approvato dal *plenum* il 10 aprile 2024 e attualmente assegnato all'esame della Camera[39] –,

---

[32] A. AMORTH, *La Costituzione italiana. Commento sistematico*, 1948, p. 62.

[33] Lo riconosce espressamente pure F. CENTORAME, *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. it. dir. proc. pen.*, 2021, p. 500.

[34] Disegno di legge n. 806 del 19 luglio 2023 d'iniziativa dei senatori Zanettin e Bongiorno, recante Modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, *smartphone* e memorie digitali.

[35] Nel Disegno di legge n. 806 del 19 luglio 2023, cit., si afferma espressamene che «il sequestro di tali dispositivi, in relazione ai dati altamente sensibili in essi contenuti, dovrebbe essere circondato da garanzie al pari delle intercettazioni e la selezione dei loro contenuti dovrebbe essere assistita da un contraddittorio tra le parti per decidere cosa sia rilevante a fini processuali».

[36] Al contrario, nel Disegno di legge n. 690 del 1° agosto 2023 d'iniziativa del senatore Scarpinato, anch'esso volto a introdurre un nuovo art. 254-*ter* all'interno del codice, si stabilisce che il pubblico ministero, quando abbia fondato motivo di ritenere che uno strumento informatico contenga dati o documenti pertinenti al reato necessari per l'accertamento dei fatti, debba richiedere al giudice competente l'autorizzazione a disporre il sequestro.

[37] L'art. 132, comma 3, del Codice della *privacy* – così come novellato dal d.lgs. 30 settembre 2021, n. 132 – attribuisce al giudice, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private, il potere di acquisiti i dati di traffico telefonico e telematico presso il fornitore dei servizi di comunicazione.

[38] Concordi sulla necessità di attribuire al giudice il potere di disporre l'apprensione del *device*, ad es., A. CHELO, *Sequestro probatorio di strumenti di comunicazione: l'imprescindibilità di una riforma*, in *Dir. pen. proc.*, 2022, p. 1588; G. LASAGNI, *Tackling phone searches in Italy and the United States*, cit., p. 394.

[39] *https://www.senato.it/leg/19/BGT/Schede/Ddliter/57327.htm*.

introducendo un sistema trifasico[40], in base al quale il pubblico ministero, qualora intenda procedere al sequestro di dispositivi, sistemi informatici o telematici o memorie digitali, deve richiedere la preventiva autorizzazione al giudice per le indagini preliminari, il quale è chiamato a operare una valutazione alla luce dei criteri di «necessità per la prosecuzione delle indagini» e «proporzionalità» dell'ingerenza.

Si è detto, inoltre, che il pubblico ministero, dopo aver eseguito l'estrazione integrale dei dati contenuti nel *device* (solitamente in triplice copia), è legittimato a trattenerla solo per il tempo strettamente necessario alla selezione delle informazioni processualmente rilevanti (*iv*). Esaurita questa operazione, egli è obbligato alla restituzione della "copia mezzo" all'avente diritto, giacché, diversamente, tale condotta realizzerebbe «una elusione ed uno svuotamento della portata dell'art. 253, comma 1, cod. proc. pen. che legittima il sequestro probatorio solo delle cose "necessarie" per l'accertamento dei fatti»[41].

La previsione di un dovere (avente, perlomeno *de iure condito*, matrice giurisprudenziale) di restituzione dell'intero materiale contenuto nella copia servente, ad eccezione dei *file* processualmente rilevanti, è senza dubbio apprezzabile, poiché volta a rendere concretamente effettivi i principi di proporzionalità e pertinenzialità che sorreggono la misura ablativa. Ne è consapevole lo stesso legislatore, tanto che nel richiamato Disegno di legge – così come approvato dal Senato – si è previsto che, una volta effettuata la duplicazione dei dati rilevanti per l'accertamento dei fatti, il pubblico ministero deve disporre senza ritardo la restituzione dei dispositivi informatici all'avente diritto.

Epperò, la scelta non è "a costo zero", specialmente se si volge lo sguardo all'istituto della revisione del processo e, più in generale, al tema dell'errore giudiziario.

A tal proposito, autorevole dottrina ha efficacemente sottolineato la «sfasatura degli orizzonti temporali che connotano il fenomeno scientifico e quello processuale», nel senso che «se la scienza e la tecnologia si caratterizzano per una dimensione di progresso illimitata, il processo penale si svolge necessariamente in un arco temporale circoscritto»[42]. Per tale ragione, l'emersione di nuove metodologie di analisi in grado di esaminare "vecchi" reperti in maniera scientificamente e tecnologicamente "nuova" va assumendo un ruolo centrale ai fini dell'applicazione dell'art. 630, comma 1, lett. c), c.p.p. In queste coordinate teoriche, un aspetto fondamentale attiene al profilo della conservazione del materiale digitale, giacché solo qualora i *file* siano stati preservati in modo adeguato potranno essere sottoposti in seguito ad approfonditi accertamenti informatici[43]. Senza considerare, in aggiunta, che il progresso tecnologico potrebbe rendere disponibili, a una distanza di tempo relativamente ravvicinata, nuove strumentazioni in grado di esaminare in maniera più approfondita i "reperti informatici".

Sotto tale profilo, allora, la restituzione della copia-clone al legittimo titolare, lo si è detto, appare coerente con la finalità di tutelare la *privacy* del soggetto ed evitare la creazione di

---

[40] *file:///C:/Users/Utente/Downloads/Sintesi-emendamento-sequestro-dispositivi-e-sistemi-informatici-o-telematici_UL.pdf*.

[41] Cass. pen., Sez. VI, 22 settembre 2020, n. 34265, cit., par. 4.

[42] M. GIALUZ, *Il giudizio di revisione*, in L. Lupária (a cura di), *L'errore giudiziario*, Milano, 2021, p. 600.

[43] Sull'importanza di tale aspetto, ancorché con riguardo ai tempi di conservazione dei campioni biologici e dei profili del DNA, v., ancora, M. GIALUZ, *Il giudizio di revisione*, cit., p. 600 s.

vere e proprie banche dati contenenti i "profili digitali" dei condannati. Nondimeno, questa procedura a vocazione garantista rischia di rivelarsi *ex post* un'arma a doppio taglio, dal momento che potrebbe inibire a monte la possibilità di svolgere una successiva analisi dei dati e, di conseguenza, la riapertura del processo. La soluzione al problema, è opportuno precisarlo, non può certo essere individuata in un generale obbligo di conservazione *ad libitum* del reperto: la *privacy* della persona coinvolta ne uscirebbe eccessivamente menomata. L'obiettivo che, per contro, dovrebbe essere perseguito è quello di predisporre un apparato normativo *ad hoc* (un po' come avvenuto per la Banca dati nazionale del DNA) che sia in grado di individuare un giusto equilibrio tra le esigenze sottese alla riservatezza (e alla *firmitas* del giudicato) e «quelle di giustizia, che premono affinché venga eliminato l'errore giudiziario scoperto grazie all'impiego di nuovi approcci scientifici o all'utilizzo di nuove tecnologie»[44].

L'ultima fase della procedura "ideale" relativa al sequestro del *device* è rappresentata, come detto, dall'esecuzione di una vera e propria perquisizione informatica (*iv*).

Sul punto, il dibattito è noto e riguarda la natura, ripetibile o meno, da attribuire all'accertamento tecnico. Mentre la dottrina si muove compatta a sostegno dell'applicabilità dell'art. 360 c.p.p.[45] (la cui violazione determinerebbe l'inutilizzabilità del materiale acquisito), la giurisprudenza di legittimità, per contro, perviene a conclusioni antitetiche, inquadrando dette attività nell'ambito degli accertamenti urgenti di cui all'art. 354 c.p.p.; una disposizione, questa, destinata a trovare applicazione tutte le volte in cui la polizia giudiziaria è chiamata a realizzare una mera raccolta di dati o, comunque, operazioni di carattere materiale che non comportano alcuna elaborazione critica di carattere scientifico[46].

In sostanza, si tratta di stabilire se la difesa abbia o meno diritto a partecipare, con un congruo preavviso, alla fase di cernita dei dati processualmente rilevanti e/o, prima ancora, alla clonazione dell'*hard disk*.

A ben vedere, le caratteristiche proprie delle attività di *digital* o *mobile forensics* consentono di affermare, al netto della distinzione tra *post mortem* e *live analisys*, la necessità di adottare uno schema simile a quello previsto all'art. 360 c.p.p. Indipendentemente dalla circostanza per cui il dispositivo sia stato trovato spento o accesso al momento dell'esecuzione del sequestro, infatti, l'operazione di creazione della copia-mezzo si caratterizza, come ebbe già a osservare autorevole dottrina, per una sorta di irripetibilità intrinseca[47]. Il rischio di un'alterazione dei dati o di una copia eseguita non a regola d'arte si rivela oggigiorno tutt'altro che ipotetico, specie a fronte di apparecchiature tecnologiche, gli *smartphone*, caratterizzate da un'elevata complessità e rispetto alle quali

[44] Testualmente, di nuovo, M. GIALUZ, *Il giudizio di revisione*, cit., p. 601.

[45] Cfr., tra i molti, L. LUPÁRIA, Computer crimes *e procedimento penale*, cit., p. 375; M. PITTIRUTI, Digital evidence *e procedimento penale*, cit., p. 105 ss.; P. TONINI, *Documento informatico e giusto processo*, cit., p. 405.

[46] La giurisprudenza sul punto è granitica. Da ultimo, Cass. pen., Sez. I, 10 giugno 2021, n. 38909.

[47] L. LUPÁRIA, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in L. Lupária – G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, cit., p. 149. Concordi, più di recente, M. DANIELE, *La prova digitale nel processo penale*, cit., p. 295 s.; M. PITTIRUTI, Digital evidence *e procedimento penale*, cit., p. 106.

pure un semplice errore in fase di "blindaggio" o di "isolamento" del *device*[48] si riverbera direttamente sulla successiva fase di copiatura. Per tale ragione, merita di essere condivisa la tesi di quanti hanno prospettato la necessità di garantire la partecipazione della difesa, con possibilità di nominare un consulente tecnico di parte, al momento in cui si realizza l'operazione di clonazione dei *bit* digitali contenuti nel *device* oggetto di sequestro[49].

Una volta prospettata la necessità di un contraddittorio a monte, duplici sono le ragioni che impongono di coinvolgere le parti private e i loro difensori anche nel corso delle attività di ricerca e individuazione dei dati processualmente rilevanti (perquisizione informatica *stricto sensu* intesa).

Viene in rilievo, in primo luogo, l'esigenza di tutelare la riservatezza dell'indagato e dei terzi coinvolti dalla misura, al fine di evitare che informazioni irrilevanti possano confluire nel compendio probatorio. In secondo luogo, non può essere sottaciuto il rischio che potrebbe derivare per l'indagato, sotto il profilo del diritto di difesa e della parità delle armi, da una selezione unilaterale e arbitraria del materiale rilevante rimessa esclusivamente in capo al pubblico ministero. Se l'obiettivo è quello di garantire un'adeguata conoscenza della documentazione processuale, giacché solo in tal modo l'accusato può valutare obiettivamente le proprie scelte processuali (in ossequio al dettame dell'art. 6, par. 3, CEDU), non v'è dubbio che un suo coinvolgimento nella fase di cernita delle informazioni risulti indispensabile.

Nell'era del "rito 2.0", però, la *discovery* non può essere intesa solamente nel senso tradizionale del termine, ovverosia come diritto dell'indagato di ricevere la comunicazione degli elementi di prova a carico e a discarico, bensì deve abbracciare un *quid pluris* rappresentato dal diritto di contribuire attivamente alla selezione del materiale probatorio. La stessa Corte di Strasburgo, in un recente arresto del 2019, ha manifestato la necessità che l'autorità inquirente instauri un dialogo con l'investigato già al momento della definizione dei modi e dei tempi di accesso al materiale informatico acquisito in sede di indagine[50].

Pur trattandosi di un atto tecnicamente ripetibile tante volte quante sono le copie-mezzo create in precedenza, l'esecuzione della perquisizione informatica dovrebbe essere preceduta, nel rispetto del canone di proporzionalità e al fine di prevenire una "bulimia investigativa", da una sorta di udienza stralcio[51] per la selezione del materiale rilevante, nella quale possa realizzarsi una "*discovery* contestuale" tra accusa e difesa. La partecipazione di

---

[48] S. GOLIN, *Questioni aperte sull'acquisizione probatoria di dati informatici*, in R. Brighi (a cura di), *Nuove questioni di informatica forense*, cit., p. 54, la quale, richiamando recenti studi di esperti informatici, esemplifica rilevando come l'accensione del dispositivo mobile per eseguire le operazioni di copiatura «modifica il contenuto dell'intero *device* rispetto a quello che aveva nel momento in cui era stato sottoposto a sequestro».

[49] M. DANIELE, *La prova digitale nel processo penale*, cit., p. 296; F. IOVENE, *Perquisizione e sequestro di* computer: *un'analisi comparatistica*, in *Riv. dir. proc.*, 2012, p. 1615.

[50] Corte edu, 4 giugno 2019, *Sigurour Einarsson c. Islanda*. A commento della pronuncia, v. L. BARTOLI, *Parità delle armi e* e-discovery *nel processo penale: quali indicazioni da Strasburgo*, in R. Brighi (a cura di), *Nuove questioni di informatica forense*, cit., p. 83 ss., alla quale si rinvia anche per più ampie e approfondite riflessioni sul tema della *electronic discovery*.

[51] Suggerisce questo percorso L. LUPÁRIA, Computer crimes *e procedimento penale*, cit., p. 375. Si mostra scettica, invece, L. BARTOLI, *Sequestro di dati a fini probatori*, cit., p. 18, per la quale se «in teoria il rimedio calzerebbe a pennello», si rischia però di cadere «su un istituto affossato dalla prassi là dove la legge l'aveva previsto», ovverosia in tema di intercettazioni telefoniche.

quest'ultima, lo si è detto, dovrebbe essere garantita a monte, anzitutto al momento della scelta del metodo utilizzato per eseguire la ricerca. Difatti, nel contesto della cd. *Electronically Stored Information*, espressione con la quale si fa riferimento alla *discovery* di informazioni contenute in ambiente digitale, è possibile ricorrere a diverse tecniche di *screening* del dato informatico, la cui scelta a favore dell'una o dell'altra appare foriera di notevoli implicazioni sul versante difensivo. Onde rendersi conto di ciò, è sufficiente considerare come a fronte della più classica e diffusa (perlomeno nel panorama italiano) metodologia di *keywords searching*[52], ossia di selezione mediante parole chiave, lo sviluppo della tecnica abbia reso oggi disponibili *software* in grado di operare selezioni sempre più accurate e capaci di aggirare i limiti di *over-inclusive* e *under-inclusive* che caratterizzano le metodologie tradizionali (cd. *Technology Assisted Review*[53]).

3. Il sequestro probatorio realizzato in ambiente *Cloud computing*: uno scenario ancora "nebuloso"

Nella prassi accade con maggiore frequenza che l'utente di un *social network* decida di archiviare tutte, o solo alcune, delle informazioni *ivi* contenute all'interno di un sistema informatico denominato *Cloud computing*. Nello stesso modo procedono, in maniera spesso automatizzata, alcune applicazioni di messaggistica istantanea, come, ad esempio, *Telegram*. In entrambi i casi, come può intuirsi, questa peculiare modalità di allocazione dei dati priva di rilevanza investigativa il *device* fisico utilizzato per l'accesso alla piattaforma.

La nuvola digitale, in via di prima approssimazione, rappresenta un moderno sistema di immagazzinamento di dati che, sfruttando lo spazio cibernetico, consente a chiunque di memorizzare i propri *bit* digitali all'interno di "nuvole virtuali" accessibili da qualunque luogo e da qualunque terminale elettronico[54]. In tal modo, perciò, le informazioni non sono più ubicate nel sistema operativo (il *software*) dello *smartphone* o del *computer*, bensì nell'"etere digitale".

Le numerose criticità sul versante investigativo legate all'impiego di questa nuova tecnologia sono già state colte dalla dottrina processualista[55] che, in proposito, è stata

[52] M. FERRAZZANO – L. SUMMA, *La selezione dei dati informatici in ambito giudiziario*, cit., p. 77. In realtà, come ricordano gli A., in determinati casi – come, ad esempio, nelle indagini per i reati di pedopornografia – si è soliti ricorrere alla comparazione mediante la cd. impronta di *hash*, cioè la comparazione tra i *file* pedopornografici contenuti in un *database* e quelli presenti nel *device*, al fine di saggiare la presenza di eventuali corrispondenze.

[53] La selezione del materiale effettuata "per parola chiave", difatti, rischia, da un lato, di includere nel compendio probatorio materiale processualmente irrilevante e, dall'altro, di escludere documenti potenzialmente rilevanti.

[54] Per un'efficace definizione, v. D. CURTOTTI, *Indagini* hi-tech, *spazio* cyber, *scambi probatori tra Stati e* Internet provider service *e "Vecchia Europa": una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 2021, p. 746, nt. 10, la quale si riferisce a un «sistema informatico di memorizzazione, archiviazione ed elaborazione dati che, grazie all'impiego di risorse *hardware* e *software* distribuite in rete, salva i dati direttamente in *Internet*. Ciò consente all'utente di accedere ai suoi dati senza aver bisogno di supporti di memorizzazione e da qualunque dispositivo».

[55] Cfr. S. ATERNO, Cloud Forensics: *aspetti giuridici e tecnici*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, cit., p. 1949 ss.; M. BONTEMPELLI, *Acquisizione di dati custoditi in ambiente* Cloud, in A. Scalfati (a cura di), *Le indagini atipiche*, cit., p. 589 ss.; S. SIGNORATO, *Le indagini digitali*, cit., p. 35-39, 199-201.

chiamata a confrontarsi con questo «tsunami digitale»[56], al fine di individuare possibili soluzioni in grado di contemperare le esigenze investigative, i principi di diritto internazionale che ruotano attorno al concetto di "sovranità" e i diritti fondamentali degli individui.

L'operazione, però, è apparsa – e appare tutt'oggi – alquanto complessa.

Si muova, per comodità espositiva, da alcuni punti fermi (*i* e *ii*), di natura prettamente tecnica, ma ricchi di implicazioni giuridiche.

i) Il concreto funzionamento della nuvola informatica rende estremamente difficile o financo impossibile determinare l'esatta collocazione territoriale dei dati *ivi* contenuti e, ciò, per un triplice ordine di ragioni.

La prima è legata al fenomeno del cd. *load balancin*g, ovverosia la migrazione costante e incontrollabile delle informazioni da un *server* a un altro (per esigenze perlopiù organizzative, tecniche, economiche e connesse a motivi di sicurezza informatica), pur localizzati in Stati diversi. Ogniqualvolta un utente esegue l'*upload* di un *file* nel *Cloud*, quello stesso *file* viene automaticamente moltiplicato e memorizzato in più *server* ubicati in Paesi diversi, al fine di proteggere i dati in caso di improvviso malfunzionamento del sistema.

In aggiunta, va considerata l'ipotesi, tutt'altro che infrequente, della cd. *loss of location* o *data loss*, espressione con la quale si allude alla "perdita di ubicazione" dei dati, causata, per l'appunto, da un continuo movimento delle informazioni. In questi casi, nessuno, men che meno il *Cloud service provider*, è in grado di identificarne l'esatta collocazione. Ciò nonostante, è bene chiarire che, in questa evenienza, il *bit* digitale risulta comunque memorizzato su un *server* che, a sua volta, è saldamente ancorato a un "computatore elettronico" ubicato in una determinata Nazione[57]. Il vero problema che si pone, dunque, è nell'impossibilità di individuare il luogo fisico nel quale è collocato il *server* che contiene il dato.

A rendere ancor più complessa l'opera di "decrittazione geografica" è, in terzo luogo, la cd. *multilocation* delle informazioni, ovverosia, la contestuale allocazione dei dati, cd. poliglotti, in più *server*.

ii) Questa nuova modalità di erogazione dei servizi di *Information Technology* – IT (si legga, *Cloud*) e le specificità del suo funzionamento hanno reso necessario lo sviluppo di nuove tecniche di *digital forensics*, al fine di «determinare le azioni eseguite su di esso o mediante esso, le modalità con cui esso è stato compiuto, e il soggetto cui lo stesso è riconducibile»[58]. A tal proposito, una delle problematiche con le quali è stata chiamata a confrontarsi la *Cloud forensics* riguarda, precisamente, la dematerializzazione e la

[56] Così, benché in altro contesto, M. GIALUZ, *La cooperazione informativa quale motore del sistema europeo di sicurezza*, in F. Peroni – M. Gialuz (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, p. 18.

[57] M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017, p. 117 s. Come sottolineato da O. POLLICINO, voce *Potere digitale*, in *Enc. dir.*, vol. V, Milano, 2023, p. 415, il cyberspazio «prima ancora che di *bit*, è costituito da infrastrutture fisiche e cavi sottomarini e quindi da una dimensione "atomica"».

[58] C. ANGLANO, Cloud forensics *e prova digitale: problematiche e soluzioni*, in *Informatica e diritto*, 2015, p. 282.

delocalizzazione del dato contenuto nella "nuvola". Dal punto di vista tecnico, infatti, quando l'utente visualizza sullo schermo del proprio *smatphone* il *file* (immagini, foto, *chat Instagram*, etc.) salvato nel *Cloud*, questo viene automaticamente "scritturato" nella RAM del *device*, dal quale viene in seguito rimosso non appena il cibernauta si disconnette dalla nuvola[59].

L'esame – pur sintetico – delle caratteristiche proprie di questi congegni informatici consente di mettere in luce le notevoli difficoltà che emergono sul piano *stricto sensu* investigativo. Nel contesto delle indagini penali transfrontaliere, come noto, una delle questioni maggiormente complesse ha da sempre riguardato l'individuazione delle norme procedurali applicabili: l'alternativa, cioè, ricade su quelle dello Stato in cui la prova è reperibile (cd. *lex loci*) o quelle dello Stato in cui la stessa verrà utilizzata (cd. *lex fori*)? Nel caso del *Cloud*, com'è evidente, la scelta appare irrilevante, giacché nessuno conosce con certezza l'ubicazione del *file*.

A fronte di prove impalpabili, dunque, occorre chiedersi quale sia la disciplina applicabile nel caso in cui la polizia giudiziaria, a seguito di un sequestro del *device*, abbia individuato la presenza di informazioni riferibili ad attività svolte sui *social network* e memorizzate in ambiente *Cloud*.

A tal proposito, è possibile distinguere diversi scenari.

Qualora l'autorità inquirente abbia ottenuto legittimamente le chiavi accesso – vuoi perché consegnate dall'indagato, vuoi perché salvate in automatico sul dispositivo, come accade spesso nel caso delle *App* di *social network* presenti sullo *smartphone*, vuoi, ancora, perché acquisite a seguito di una perquisizione – non sembrano profilarsi questioni in tema di *transborder access*. Pur in mancanza del consenso manifestato dal legittimo titolare, infatti, la circostanza che l'autorità inquirente sia riuscita ad ottenere legittimamente alle chiavi di accesso consente, in virtù del cd. *power of disposal*[60], di applicare la legge dello Stato in cui il contenuto digitale è visualizzato[61].

Più complesso è, invece, stabilire se, come e in quale misura gli inquirenti possano acquisire tali informazioni nel caso in cui non siano riusciti a entrare in possesso delle *password* ovvero a forzare il sistema mediante l'impiego di *software ad hoc*. In ragione della *unterritoriality* che caratterizza il funzionamento dei *Cloud*, i meccanismi tradizionali di mutua assistenza si rivelano infruttuosi, non potendo operare laddove non si è in grado di

[59] C. KARAGIANNIS – K. VERGIDIS, *Digital Evidence and Cloud Forenscs: Contemporary Legal Challenges and the Power of Disposal*, in *Information*, 22 aprile 2021, p. 6.

[60] Si tratta di un criterio proposto nel contesto sovranazionale e, più in particolare, nell'ambito della DIREZIONE GENERALE DEL CONSIGLIO D'EUROPA, *Discussion paper on Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, 10 agosto 2010, per superare i limiti connessi alla "delocalizzazione" del *Cloud computing*. In sintesi, si afferma che il potere di accedere a dati contenuti nelle "nuvole digitali" spetta «a chi detiene il diritto di modificare, cancellare, sopprimere o rendere inutilizzabili i dati o, ancora, di escludere chiunque altro da ogni accesso ai medesimi» (G.M. RUOTOLO, Hey! You! Get Off My Cloud! *Accesso autoritativo alle nuvole informatiche e diritto internazionale*, in *Arch. pen.* web, 2013, p. 862).

[61] Per le medesime conclusioni, v. B.J. KOOPS – M. GOODWIN, C*yberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law*, in *Tilburg Law School Research paper*, 2014, 5, p. 63; e, nel panorama nazionale, *in primis*, S. SIGNORATO, *Le indagini digitali*, cit., p. 167. Concorde pure A. MANGIARACINA, *Nuovi scenari nell'accesso transfrontaliero alla prova "elettronica"*, in V. Militello – A. Spena (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, cit., p. 437.

identificare con certezza lo Stato al quale inviare la richiesta di cooperazione internazionale (si legga, rogatoria).

A tal proposito, l'*European Judicial Cybercrime Network*[62] e la dottrina più accorta[63] hanno dato conto dell'esistenza di prassi *in absentia legis* sviluppatesi in numerosi Stati europei (e non solo), in forza delle quali l'autorità procedente si rivolge direttamente al gestore della piattaforma per conoscere la collocazione fisica del *server* nel quale sono ubicati i dati. Così facendo, tuttavia, l'individuazione della legge processuale applicabile è rimessa *in toto* a soggetti che operano sulla base di interessi privatistici, in palese contrasto con il canone del giudice naturale precostituito per legge (art. 25 Cost.). Si è già detto, peraltro, come, in simili evenienze, neppure il *Cloud service provider* sia in grado di conoscere l'esatta collocazione dei *file*, con la conseguenza che una richiesta tal fatta appare sostanzialmente inutile. L'unica risposta corretta che dovrebbe essere fornita dal *provider* è un semplice, ma sincero, "non so".

Nelle situazioni di "perdita di posizione", pertanto, il principio di territorialità – che imporrebbe di individuare la legge applicabile a seconda del luogo fisico in cui sono memorizzati i dati – non sembrerebbe poter trovare applicazione[64]. È questa, del resto, la tesi accolta dal *Cybercrime Convention Committee* laddove afferma che l'attività di indagine penale volta alla ricerca di dati ubicati nei *Cloud* non provoca alcuna ingerenza nel principio di sovranità statale[65]. Si osserva, in particolare, che nell'ipotesi di *loss of location* l'ordinamento perderebbe interesse alla tutela della propria sovranità territoriale, poiché il rapporto tra le informazioni contenute nel *Cloud* e lo Stato risulterebbe meramente accidentale.

Questo approccio, tuttavia, non appare affatto convincente. Anche laddove si dimostrasse questa teorica carenza di interesse[66], permarrebbe in capo a ogni Nazione l'esigenza di proteggere le proprie infrastrutture (e i dati che *ivi* circolano), alle quali – seguendo tale approccio – sarebbe consentito, sempre e comunque, l'accesso agli agenti stranieri.

Se si accoglie questa prospettiva, perciò, occorre individuare uno strumento che consenta agli inquirenti di acquisire i dati a prescindere dalla loro esatta localizzazione, ma nel rispetto della sovranità statale. La soluzione, a ben vedere, non può che essere ricercata nel contesto della cooperazione internazionale ed europea, giacché solamente accordi di diritto sovraordinato possono legittimare una (volontaria) limitazione della sovranità a favore di

---

[62] EUROPEAN JUDICIAL CYBERCRIME NETWORK, *7h Plenary Meeting – Eurojust*, 14-15 novembre 2019.

[63] M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, cit., p. 1891 ss.; S. SIGNORATO, *Le indagini digitali*, cit., p. 200.

[64] CYBERCRIME CONVENTION COMMITTEE (T-CY), C*riminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY Final report of the T-CY Cloud Evidence Group*, 16 settembre 2016, par. 43.

[65] CYBERCRIME CONVENTION COMMITTEE (T-CY), *Transborder access and jurisdiction: What are the options?*, 6 dicembre 2012, par. 134.

[66] Dubbi in proposito sono manifestati da U. SIEBER – C.W. NUEBERT, *Investigaciones transnacionales de crìmenes en el ciberspacio: retos a la sobranìa nacional*, in A. Nieto Martìn – B. Garcìa Moreno (a cura di), *Ius puniendi y Global Law. Hacia un dereho penal sin estado*, Valencia, 2019, p. 325.

una più efficace attività penale investigativa[67]. Ed è proprio in questa direzione, d'altro canto, che si collocano il Regolamento europeo relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale e il II Protocollo addizionale alla Convenzione sulla criminalità informatica in tema di "cooperazione rafforzata e divulgazione di prove elettroniche. In entrambi i provvedimenti – ancorché aventi ambiti operativi differenti – il legislatore ha preso atto della necessità, della quale si darà conto più approfonditamente in seguito, di coinvolgere gli *Internet service provider* nella concreta esecuzione delle indagini preliminari. Questi ultimi, di fatto, sono i veri titolari del potere di disposizione dei dati che, a ben vedere, dovrebbe rappresentare, nell'ambito del *Cloud computing*, l'unico criterio sul quale basare la cooperazione giudiziaria[68].

Sul punto, però, occorre muoversi con una certa cautela.

Da un lato, va accolta con favore l'idea di disciplinare in maniera dettagliata la cooperazione diretta tra organi inquirenti e fornitori di servizi *Internet*[69], a prescindere dalla ubicazione dei dati, superando così il (discutibile) modello invalso nella prassi della cd. *voluntary disclousure* – in base al quale ciascuna azienda decide, di volta in volta, se collaborare o meno con l'autorità richiedente – e garantendo un quadro giuridico chiaro, non frammentato e indubbiamente più aderente al principio di uguaglianza[70]. Dall'altro, però, il coinvolgimento dei giganti dell'*hi-tech* nell'*iter* procedimentale impone di vigilare con attenzione sull'effettivo rispetto delle garanzie fondamentali di tutti i soggetti coinvolti.

4. *Nemo tenetur se detegere* e apprensione dei codici di accesso

Se lo *smartphone* e gli altri dispositivi elettronici di uso quotidiano costituiscono, a tutti gli effetti, una prosecuzione esterna del corpo umano, è agevole comprendere la ragione per la quale ciascun cibernauta è sempre più propenso a impostare sistemi di sicurezza (*password* o codici di accesso) in grado di proteggere le informazioni *ivi* contenute.

Questa scelta – del tutto legittima e, anzi, auspicabile – rischia, però, di rappresentare un ostacolo talvolta insormontabile per lo svolgimento delle indagini penali. Nell'intento di accedere al contenuto del *device*, infatti, la polizia giudiziaria (*rectius*, l'esperto) potrebbe trovarsi di fronte all'impossibilità di decifrare o forzare il sistema informatico, stante l'elevato grado di difesa offerto dalle moderne tecniche di protezione, in grado di inibire anche i più sofisticati *tools* di decriptazione. Ancorché l'art. 354, comma 1-*bis*, c.p.p. consenta all'"autorità perquirente" di attuare un vero e proprio «*cracking* legalizzato»[71] mediante l'impiego di strumenti atti a superare eventuali ostacoli di natura informatica, il

[67] Non appaiono condivisibili, dunque, gli *unilateralist approaches* adottati da numerosi Stati europei (e non solo) nelle ipotesi di *loss of location*, consistenti nel dettare norme di procedura penale interna che obbligano i fornitori dei servizi attivi sul territorio nazionale a divulgare i dati sotto il loro controllo, indipendentemente dal luogo nel quale questi sono archiviati, sotto minaccia di pesanti sanzioni di carattere economico. Si veda, ad esempio, l'art. 88-*ter* del codice di rito belga.

[68] In questo senso, v. anche F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Proc. pen. giust.*, 2017, p. 186.

[69] Dello stesso avviso sono M. GIALUZ – J. DELLA TORRE, *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022, p. 282.

[70] La libertà in capo al *provider* di scegliere se collaborare o meno con gli inquirenti può difatti ingenerare profonde e ingiustificate disparità tra imputati.

[71] La felice espressione è di L. MARAFIOTI, Digital evidence *e processo penale*, cit., p. 4516.

rischio di una stasi investigativa deve ritenersi, in concreto, tutt'altro che remoto. Questo timore, del resto, è stato plasticamente evidenziato dalla dottrina nordamericana che lo ha riassunto nell'espressione «*fear of going dark*»[72], ovverosia la paura di cadere nel buio investigativo a causa dell'impossibilità di accedere a dati e informazioni essenziali per la prosecuzione dell'*iter* procedimentale.

Se le considerazioni appena svolte possono senz'altro valere con riguardo a tutti i casi in cui l'azione investigativa sia ostacolata dalla presenza di *password*, nel caso che ci occupa, però, i problemi assumono una complessità ancor maggiore. Nell'ambito dei *social network*, infatti, gli inquirenti potrebbero essere chiamati a svolgere un'operazione di doppia decrittazione, giacché è ben possibile che l'utente (specialmente in contesti di criminalità economica e organizzata) abbia impostato le credenziali di accesso anche per collegarsi alle applicazioni che gestiscono l'utilizzo delle piattaforme.

Alla luce del quadro appena descritto, non v'è chi non veda come la necessità di garantire la prosecuzione delle indagini si ponga in aperto contrasto con l'esigenza di garantire i diritti dell'indagato, quali, per tutti, il diritto al silenzio e a non autoincriminarsi. A fronte dell'impossibilità di accedere al contenuto del sistema informatico e degli *accounts social*, occorre chiedersi se l'ordinamento possa imporre un obbligo, penalmente sanzionato, all'accusato di rivelare i propri codici di sicurezza, nonché quale debba essere il contegno *stricto sensu* procedimentale tenuto dalla polizia giudiziaria o dal pubblico ministero al momento della richiesta delle credenziali di accesso. Si potrebbe disquisire, in proposito, di una sorta di «*social network privilege*»[73] per descrivere il diritto dell'utente di non collaborare con l'autorità nella ricerca delle informazioni private contenute nei propri *social-accounts*?

Si proceda con ordine.

Nel cercare di bilanciare le opposte esigenze in gioco, l'art. 19, comma 4, della Convenzione di Budapest consente agli Stati contraenti di adottare misure legislative e di altra natura che risultino necessarie per consentire alle autorità competenti «di ordinare ad ogni soggetto che abbia conoscenza del funzionamento del sistema informatico o delle misure utilizzate per proteggere i dati informatici in esso contenuti, di mettere a disposizione tutte le informazioni ragionevolmente necessarie per consentire» la perquisizione e il sequestro di detti apparati.

L'impiego della locuzione soggettivizzante «*any person*» ha indotto numerosi ordinamenti nazionali a introdurre casi di *disclousure requirement*, presidiando l'eventuale diniego alla consegna della *password* anche con sanzioni di carattere penale[74]. L'adozione di dette legislazioni, a ben vedere, è stata resa possibile anche in virtù di una normazione a livello europeo che, sul punto, non brilla certo per chiarezza espositiva. Il riferimento va all'art. 7 della Direttiva 2016/343/UE in tema di presunzione di innocenza e al relativo considerando

[72] Per tutti, O.S. KERR, *Compelled Decryption and the Privilege Against Self-Incrimination*, in *Texas Law Review*, 2018, p. 767 ss.

[73] L'icastica espressione è presa a prestito da J.G. BROWNING, *Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, in *Science and Technology Law Review*, 2017, p. 486.

[74] Ad es., Belgio, Croazia, Francia, Irlanda e Regno Unito.

(n. 29)[75]. Con tale disposizione, il legislatore europeo, come messo in luce dalla più attenta dottrina[76], ha sostanzialmente recepito quell'orientamento della giurisprudenza di Strasburgo secondo cui il diritto a non autoincriminarsi non può trovare applicazione con riguardo a quelle prove ottenute mediante l'impiego di «*compulsory powers*» che «esistono indipendentemente dalla volontà dell'imputato», come, ad esempio, l'analisi dell'aria alveolare espirata, del sangue, delle urine o dei tessuti corporei destinati all'esecuzione della prova del DNA (cd. prove volontà indipendenti)[77]. Pur elencando apprezzabilmente le tipologie di "informazioni" che non rientrano nel campo di applicazione del privilegio, non è chiaro se tale catalogo costituisca o meno un *numerus clausus*, consentendo, in linea teorica, di escludere tutti quei dati processualmente rilevanti non espressamente menzionati al considerando n. 29, tra i quali potrebbero essere annoverati i codici di sblocco dei dispositivi elettronici[78].

Prima di esaminare più nel dettaglio gli aspetti problematici sul versante italiano, occorre muovere da alcune considerazioni di carattere preliminare.

In primo luogo, la rilevanza assunta in questa materia dal *nemo tenetur se detegere* – nei termini che si illustreranno a breve – si giustifica, a differenza di quanto si è cercato di sostenere nel contesto della *false friends technique*, alla luce del fatto che la richiesta della *password* da parte dell'autorità procedente avviene "alla luce del sole", instaurandosi così un rapporto diretto e immediato (si legga, non mediato) con il dichiarante; requisito, quest'ultimo, che, come si è visto, costituisce il presupposto per l'operatività della garanzia *de qua*.

In secondo luogo, mette conto osservare che l'oggetto di tutela del diritto al silenzio, in questo caso, è rappresentato dall'atto di rivelazione dei codici informatici. La notazione non è di poco momento, giacché tale comportamento potrebbe essere qualificato, di per sé, come "neutro", non implicando in alcun modo né una dichiarazione confessoria, né, tantomeno, un comportamento autoincriminante[79]. Non sfugge, però, come pure un semplice atto "neutro" possa incidere sul *privilege against self incrimination*, perlomeno laddove quest'ultimo venga interpretato in senso ampio, cioè come diritto a non collaborare con l'accusa nello svolgimento delle indagini a proprio carico. L'apprensione del sistema informatico ad opera della polizia giudiziaria, infatti, si qualifica come un'operazione investigativa complessa, nel contesto della quale la richiesta di consegna della *password*

[75] Sulla quale, v., per tutti, J. DELLA TORRE, *Il paradosso della direttiva sul rafforzamento della presunzione di innocenza e del diritto di presenziare al processo: un passo indietro rispetto alle garanzie convenzionali?*, in *Riv. it. dir. proc. pen.*, 2016, p. 1835 ss.

[76] J. DELLA TORRE, *Il paradosso della direttiva sul rafforzamento della presunzione di* innocenza, cit., p. 1876.

[77] Corte edu, 17 dicembre 1996, *Saunders c. Regno Unito*, par. 69; Corte edu, 11 luglio 2006, *Jalloh c. Germania*; Corte edu, 29 giugno 2007, *O'Halloran e Francia c. Regno Unito*.

[78] Sul punto, v. A. PIVATY e altri, *Opening Pandora's box: The Right to Silence in Police Interrogations and the Directive 2016/343/EU*, in *New Journal of European Criminal Law*, 2021, p. 339.

[79] Questa impostazione è stata recentemente sostenuta dalla Corte Suprema belga nella sentenza *Hof van Cassatie*, 4 febbraio 2020, P.19.1086.N, reperibile al sito *www.stradalex.it*.

assume la funzione di atto prodromico all'acquisizione di informazioni potenzialmente *contra se*[80].

Ciò chiarito, occorre analizzare, anzitutto, il caso in cui l'autorità inquirente richieda all'indagato di rivelare il proprio *nickname*. Più nel dettaglio, si pone il problema di stabilire se questa nuova forma di "identità digitale" – sovente impiegata nei *social network* – debba essere o meno ricompresa nei concetti di «generalità» dell'indagato o «quant'altro può valere a identificarlo» previsti all'art. 66, comma 1, c.p.p., rispetto ai quali egli ha obbligo di verità, non potendo opporre – perlomeno secondo l'opinione dottrinale dominante[81] – l'esercizio del diritto al silenzio. A tal fine, mette conto osservare come l'interrogativo permanga anche a seguito dell'entrata in vigore della Direttiva 2016/343/UE, il cui considerando n. 26 si limita ad affermare che il diritto al silenzio e il diritto di non autoincriminarsi devono ritenersi applicabili alle domande riguardanti il reato asseritamente commesso dall'indagato e non, ad esempio, a quelle relative all'«identificazione» di quest'ultimo.

Duplici sono le interpretazioni prospettate in letteratura.

Facendo leva su un'esegesi evolutiva, accreditati studiosi hanno sostenuto che il concetto di identità personale cui si riferisce la disposizione codicistica vada inteso in senso ampio, tale da ricomprendevi anche le nuove forme di "anagrafica virtuale"; di talché, l'imputato non potrebbe avvalersi dello *ius tacendi*[82]. Altra postura dottrinale, per contro, ha negato con fermezza la possibilità di imporre un tale obbligo, specialmente a fronte di indagini penali volte ad accertare la commissione di reati informatici; in queste ipotesi, infatti, la rivelazione del proprio *nickname* equivarrebbe a un vero e proprio contegno autoincriminante che, in quanto tale, risulta incoercibile[83].

Quest'ultima impostazione, a ben vedere, appare preferibile. In effetti, il ricorso a un'esegesi "tecnologicamente evoluta" del dettato normativo, ancorché sovente necessaria per far fronte alle innumerevoli sfide poste dall'innovazione digitale, parrebbe contrastare con la regola aurea d'interpretazione in base alla quale la limitazione di un diritto fondamentale non può desumersi da una lettura estensiva della legge. Per di più, la scelta a favore del silenzio dovrebbe ritenersi giuridicamente consentita in tutte quelle ipotesi nelle quali l'esternazione delle proprie generalità equivarrebbe all'ammissione di colpevolezza, come nel caso di imputazioni inerenti all'art. 494 c.p.[84].

---

[80] In questo senso, v. pure A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici… e non solo*, in *Proc. pen. giust*., 2021, p. 739.

[81] L'art. 64, comma 2, lett. c), c.p.p., infatti, riconosce all'interrogato la facoltà di non rispondere, «salvo quanto disposto dall'art. 66, comma 1». A favore di tale esegesi, v., per tutti, O. DOMINIONI, sub *Art. 66-68*, in *Commentario del nuovo codice di procedura penale*, diretto da E. Amodio – O. Dominioni, Milano, 1989, p. 411.

[82] Ha prospettato, per prima, questa esegesi, S. SIGNORATO, *Le indagini digitali*, cit., p. 34 s., la quale giustifica l'assunto facendo leva su «una lettura evolutiva [del dettato normativo] alla luce della tecnologia».

[83] Per questa opinione, v., ad es., A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio*, cit., p. 736; C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, 2019, p. 1167 ss.

[84] La tesi (qui condivisa) che sostiene l'operatività del diritto al silenzio e al mendacio sulle proprie generalità nel caso in cui ciò risulti funzionale all'esercizio del diritto di difesa è stata prospettata da O. MAZZA, *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, Milano, 2004, p. 111 ss.

Per quanto concerne, poi, il tema delle credenziali di accesso (*password*), occorre anzitutto distinguere il caso in cui la polizia giudiziaria ne richieda espressamente la consegna, dall'ipotesi nella quale essa sia spontaneamente offerta dall'indagato.

Con riguardo a quest'ultima, a ben vedere, non sembrano venire in rilievo aspetti problematici di alcun tipo, giacché egli sceglie liberamente di condividere il proprio bagaglio conoscitivo con l'autorità inquirente. Una questione di non poco conto, però, riguarda il controllo circa l'effettiva volontarietà della condotta tenuta dall'imputato. Se è vero che il confine tra spontaneità, sollecitazione e coercizione appare, in molti casi, assai labile, è opportuno che il giudice effettui un controllo serrato *ex post* circa l'intenzionalità di tale dichiarazione. A questo proposito, è auspicabile che la consegna dei codici avvenga sempre in presenza del difensore, come, ad esempio, nel corso dell'interrogatorio. In tal modo, andrebbe grandemente scemando il rischio che gli inquirenti realizzino un'indebita pressione psicologica sul dichiarante[85].

A una diversa conclusione dovrebbe giungersi qualora sia direttamente l'organo d'accusa a richiedere all'indagato la consegna della *password*. In questa circostanza, egli non può essere costretto a rivelare la chiave per accedere ai propri *accounts social*. Benché questo atto, come detto, non rappresenti una vera e propria autoincriminazione – l'imputato, difatti, si limita a fornire informazioni per entrare in possesso di materiale probatorio potenzialmente sia *in favor* che *contra se* – un'esegesi estensiva del *privilege* osta a una coazione in tal senso. Il *nemo tenetur se detegere* impone, altresì, che la richiesta eventualmente avanzata dagli inquirenti sia preceduta, a pena di inutilizzabilità, dall'avvertimento della facoltà di non rispondere *ex* art. 64, comma 3, lett. b), c.p.p. (in combinato congiunto con l'art. 350, comma 1, c.p.p.)[86].

4.1 *Touch ID* e *Face ID*: linee evolutive del diritto al silenzio nell'era della biometria

Dette considerazioni potrebbero essere destinate a mutare con riguardo alle chiavi di sicurezza biometriche. I moderni artefatti comunicativi, come noto, permettono all'utente di utilizzare nuove tecniche di protezione dei dati contenuti all'interno dei propri dispositivi e dei propri *accounts*: si pensi, ad esempio, alle impostazioni degli *smartphone* che consentono di predisporre quali codici-sblocco le impronte digitali, la retina oculare o il riconoscimento facciale.

---

[85] Pure alcuni appartenenti alla magistratura requirente sembrano prediligere questo *modus procedendi* proprio al fine di garantire la volontarietà della dazione (v., ad es., F. CAJANI, *Le "nuove frontiere" dell'investigazione digitale alla luce della legge n. 48/2008, ovvero: quello che le norme (ancora) non dicono*, in AA.VV., Cyber forensics *e indagini digitali*, Torino, 2021, p. 551).

[86] In tal senso v., *ex plurimis*, L. LUPÁRIA, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, cit., p. 158-160; S. SIGNORATO, *Le indagini digitali*, cit., p. 35; L. MARAFIOTI, Digital evidence *e processo penale*, cit., p. 1466. Isolata è, invece, la posizione assunta da P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, cit., p. 1629, nt. 218, per la quale «l'interpretazione riferita non pare convincente; è vero, infatti che la collaborazione non può essere imposta, ma è altrettanto vero che l'avvertimento del diritto al silenzio è garanzia delineata con riferimento agli atti di indagine in cui l'indagato interviene, non per propria scelta, come dichiarante. Appare significativo, d'altro canto, che l'avvertimento in questione non sia previsto per l'ipotesi delle dichiarazioni spontanee rese dall'indagato alla polizia giudiziaria ai sensi dell'ultimo comma dell'art. 350 c.p.p.».

L'attivazione, in dette ipotesi, del privilegio contro l'autoincriminazione dipende, a ben riflettere, dal peso che si intenda riconoscere, nell'attuale panorama socio-tecnologico, alla tradizionale distinzione relativa al *modus partecipandi* dell'accusato all'attività investigativa, ovverosia quale "organo" o quale "oggetto" di prova[87]. Con la prima locuzione, come risaputo, si allude all'insieme delle facoltà attribuite all'indagato – espressone del diritto di autodifesa – con le quali egli apporta volontariamente, coscientemente e in maniera attiva un contributo conoscitivo al processo. Quanto alla seconda, per contro, egli viene in considerazione come mero oggetto dell'osservazione giudiziale, assumendo in tal modo la qualifica di soggetto passivo dell'accertamento. Il differente ruolo ricoperto dall'indagato nelle due ipotesi incide sul campo di applicazione del diritto al silenzio: quest'ultimo può (e deve) operare solo qualora l'interessato esprima un contributo attivo nell'istruzione probatoria.

Volendo calare tali categorie nel contesto in esame, risulta *prima facie* evidente che l'esercizio di un potere fisico-coercitivo da parte della polizia giudiziaria per costringere l'indagato a sbloccare il proprio dispositivo non provochi alcuna interferenza con il divieto di non autoincriminarsi[88]. Il soggetto, al pari di quanto avviene nel caso di una perquisizione, di un'ispezione o di un prelievo coattivo di materiale biologico[89], è chiamato a soggiacere al legittimo esercizio di un potere pubblico, fornendo così un mero contributo passivo all'accertamento dei fatti[90]. In questi casi, l'indagato, per dirla con le parole della Suprema corte, è un'entità fisica che diviene oggetto di ricerca probatoria, a prescindere da una qualche forma di collaborazione: poiché «non occorre alcuna sua attivazione fisica per lo svolgimento dell'indagine» egli non può «impedire l'emergere di elementi di prova dal proprio corpo»[91].

Dubbi, casomai, potrebbero sorgere con riguardo a una possibile violazione della libertà personale del soggetto sottoposto al "prelievo forzoso" della *password*. In effetti, qualora il contenuto dell'art. 13 Cost. sia inteso (anche) come libertà fisica di movimento in assenza di costrizioni esterne (si legga, «poteri coercitivi implicanti la sottoposizione, sia pur momentanea, a stato detentivo»[92]), l'immobilizzazione del soggetto, seppur per il brevissimo

---

[87] La messa a punto di tale classificazione si deve a E. FLORIAN, *Delle prove penali*, vol. II, Milano, 1924, p. 9.

[88] È opportuno precisare come nessuna rilevanza assuma, in questo contesto, il disposto dell'art. 349, comma 2, c.p.p., a mente del quale la polizia giudiziaria è autorizzata a svolgere nei confronti della persona indagata «rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti». La disposizione, infatti, limita l'impiego di tali dati con esclusivo riferimento all'identificazione del soggetto, risultando perciò precluso qualsiasi altro utilizzo. Nello stesso senso, v. già A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio*, cit., p. 739.

[89] Con specifico riguardo al tema dell'accesso al corpo dell'imputato, la dottrina più accreditata ha sottolineato come «il canone del *nemo tenetur* assuma rilievo diretto esclusivamente con riferimento alle informazioni che possono venir alla luce per effetto di una scelta volontaria dell'imputato, mentre potrà avere rilevanza meramente indiretta per gli atti in cui l'imputato è oggetto di accertamento». Con riguardo a questi ultimi – si conclude – l'indagato «si trova in una posizione di soggezione, rispetto alla quale si configura una vera e propria *servitus iustitiae*» (M. GIALUZ, *Radiologia e accertamenti medici coattivi: il difficile equilibrio tra libertà della persona ed esigenze di prova*, in *Riv. it. dir. proc. pen.*, 2012, p. 562).

[90] Di questa opinione è, ad es., F.N. RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'auto-incriminazione*, in *Cass. pen.*, 2022, p. 890.

[91] Così, benché in altro contesto, Cass. pen., Sez. I, 16 ottobre 1990, Andraous.

[92] G. AMATO, *Individuo e autorità nella disciplina della libertà personale*, Milano, 1967, p. 23 s.

lasso di tempo funzionale all'apprensione delle credenziali, rischia di risolversi in una menomazione della suddetta garanzia. Una menomazione che, *in absentia legis*, deve ritenersi, allo stato attuale, illegittima.

A differenti conclusioni dovrebbe giungersi (con riguardo all'ipotizzata violazione del *privilege*), come si accennava, qualora si intenda prediligere un approccio "moderno" al tema della collaborazione processuale dell'imputato, abbandonando definitivamente il binomio coazione "propria" e "impropria", a favore di un'estensione a 360 gradi del *nemo tenetur se detegere*[93]. Del resto, la miglior dottrina, benché con riguardo al tema degli accertamenti medici coattivi (terreno di elezione per gli studi volti a saggiare la portata estensiva del *privilege*), ha osservato come il corpo umano, a seguito dell'evoluzione della scienza e della tecnica, abbia «acquisito una peculiare e inedita valenza cognitiva», essendosi ampliata notevolmente la capacità di estrapolare da esso informazioni processualmente rilevanti, «a prescindere dalla parola del suo titolare»[94]. In quel contesto, si è messa in luce la necessità di riconoscere all'indagato (o al terzo sottoposto alla misura) «diritti specifici, che fungano da scudo giuridico volto a proteggere l'individuo rispetto alle pretese conoscitive dell'autorità»[95]. Dette considerazioni non possono che essere condivise. I più autorevoli commentatori, del resto, hanno sottolineato come il *nemo tenetur*, in un contesto sociale e investigativo sempre più digitalizzato e dematerializzato, debba essere interpretato in senso rigoroso e applicato ogniqualvolta l'indagato è oggetto di prova o, più correttamente, «fonte di dati»[96].

Cercando di calare quanto appena osservato nel campo di interesse, vanno assumendo un certo vigore interpretativo il già richiamato art. 7 della Direttiva 2016/343/UE e il relativo considerando esplicativo (n. 29), nella parte in cui prevedono che il campo di applicazione del diritto a non autoincriminarsi non si estenda alle prove che «esistono indipendentemente dalla volontà dell'imputato». Ipotesi, queste ultime, ricondotte pacificamente nell'ambito di quelle attività processuali dirette nei confronti dell'imputato "oggetto" passivo di prova.

Ebbene, appare forse eccessivamente semplicistico equiparare *sic et simpliciter* le situazioni appena descritte.

Non convince, innanzitutto, l'idea di qualificare i dati biometrici alla stregua di elementi che esistono a prescindere dalla volontà dell'imputato, giacché questi, a differenza del campione sanguineo, sono stati "creati" *ad hoc* proprio da quest'ultimo, con il fine di proteggere informazioni a carattere riservato. Per di più – ed è questo un punto non privo di rilievo – in entrambe le ipotesi (*password* tradizionale e *password* biometrica) l'atto di rivelazione, lo si è detto, rappresenta il prodromo di una futura acquisizione di materiale potenzialmente *contra se*. Da questo punto di vista, perciò, parrebbe irragionevole (art. 3 Cost.) trattare diversamente situazioni che, in concreto, hanno il medesimo impatto

[93] Sembra collocarsi in questa prospettiva A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio*, cit., p. 740, per la quale tale distinguo non è «in alcun modo applicabile alle chiavi di protezione dei sistemi informatici».

[94] M. GIALUZ, *Radiologia e accertamenti medici coattivi*, cit., p. 559 s.

[95] Così, ancora, M. GIALUZ, *Radiologia e accertamenti medici coattivi*, cit., p. 560.

[96] Nuovamente, M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 57.

pregiudizievole sull'esercizio del diritto al silenzio. Se vi è, dunque, una sorta di "equivalenza funzionale" tra i due sistemi di sblocco – giacché entrambi mirano a proteggere i contenuti presenti nelle piattaforme da intrusioni indebite da parte di terzi (e, perciò, anche dell'autorità statale) – non si vede perché tali situazioni debbano soggiacere a discipline e limiti differenziati. In altre parole, sembra che la scelta di limitare il campo di applicazione del *privilege* a seconda del metodo e del formato di decrittazione utilizzato (*password* alfanumerica o *Touch ID-Face ID*) risulti lesiva del principio di uguaglianza, generando così risultati iniqui.

Ulteriori e convincenti conferme circa la bontà dell'approccio qui proposto provengono, ancora una volta, dall'analisi comparata e, più in particolare, dal dibattito giurisprudenziale e dottrinale sviluppatosi nel contesto nordamericano in merito alla legittimità di un *search warrant* che consenta agli inquirenti di operare un rilievo forzoso delle impronte digitali e biometriche dell'indagato (cd. *compelled decrypton*)[97]. Il tema, più in particolare, ruota attorno all'estensione applicativa che si intenda riconoscere al V Emendamento che, nel prevedere un vero e proprio *privilege against self incrimination*, stabilisce che «*no person shall be […] compelled in any criminal case to be a witness against himself*».

Nella piena consapevolezza delle differenze che intercorrono tra il modello processuale italiano e quello d'oltreoceano, va osservato come le argomentazioni spese in quella sede offrano comunque utili spunti di riflessione. Nel contesto americano, infatti, è attualmente pendente un fervente contrasto in sede pretoria e dottrinale tanto in merito all'applicabilità del V Emendamento con riguardo alla rivelazione forzosa delle *password* alfanumeriche[98], quanto in relazione alle più moderne forme di *Touch ID-Face ID*.

A quest'ultimo proposito, la maggior parte delle Corti Federali vanno avallando la tesi di un'irrilevanza del *privilege* in merito alle attività investigative di *compulsion biometric encryption*: il riconoscimento dell'iride, del volto o il prelievo forzoso dell'impronta digitale – si sostiene – non rappresentano comportamenti *strcto sensu* comunicativi[99], bensì mere "scansioni del corpo umano"[100]. L'indagato, in questa prospettiva, è qualificato alla stregua

[97] La letteratura che si è sviluppata sul tema è già imponente. Tra i primi commentatori, v., autorevolmente, S.W. BRENNER, *Encryption, Smart Phones, and the Fifth Amendment*, in *Whittier Law Review*, 2012, p. 525 ss. e O.S. KERR, *Compelled Decryption and the Privilege Against Self-Incrimination*, cit. Cfr. anche L. SACHAROFF, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, in *Fordham Law Review*, 2018, p. 203 ss.; D.W. OPDERBECK, *The Skeleton in the Hard Drive: Encryption and the Fifth Amendment*, in *Florida Law Review*, 2018, p. 883 ss.

[98] A favore dell'operatività del V emendamento, in ragione della natura "dichiarativa" e potenzialmente auto-incriminante dell'atto di rivelazione, v., *ex multis*, *Stati Uniti c. Doe*, 670 F.3d 1335, 1346 (lith Cir. 2012); *Stati Uniti c. Pittman*, 367 498, 518 (2021); *Lewis c. Stati Uniti*, 571 S.W.3d 498, 501-03 (Ark. Ct. App. 2019); *Commonwealth c. Davis*, 220 A.3d 534, 543 (Pa. 2019); *Stati Uniti c. Andrews*, 243 N.J. 447, 466 (2020). *Contra*, tra le molte, *Mickelson c. Stati Uniti*, No. 78513, 2020 WL 5837973, (Nev. Sept. 30, 2020); *Stati Uniti c. Stahl*, 206 So.3d 124, 127 (Fla. Dist. Ct. App. 2016); *Mickelson c. Stati Uniti*, No. 78513, 2020 WL 5837973, (Nev. Sept. 30, 2020); *Commonwealth c. Jones*, 117 N.E. 3d 702, 714 (Mass. 2019). Cfr., *amplius*, A. GILLESPIE – J. SHURSON – S. MASON, *Encrypted data*, in S. Mason – D. Seng (a cura di), *Electronic Evidence and Electronic Signatures*, Londra, 2021, p. 397 ss. e, spec., p. 414 ss.

[99] E, dunque, in base alla dottrina *Fisher*, non sono protetti dal *privilege*: *Fisher c. Stati Uniti*, 425 U.S. 391, 409 (1976).

[100] A favore di questa esegesi, v., *ex plurimis*, *Stati Uniti c. Diamond*, 905 N.W.2d 870, 872 (Minn. 2018); *Stati Uniti c. Barrera*, 415 F. Supp. 3d 832, 842 (N.D. Ill. 2019). Concordi, in dottrina, L. PHELPS, *It Is Only Fingerprint: Biometric Compulsion and the Fifth Amendment*, in *UMKC Law Review*, 2020, p. 479, 486, per

di una semplice fonte passiva di prova, al pari di quanto accade nelle ipotesi di prelievo forzo di campioni salivari o sanguinei, non essendo richiesto «l'accesso ai contenuti della sua mente»[101], requisito necessario per l'operatività del *nemo tenetur*. Evidenti sono le contiguità con la richiamata distinzione, di matrice italiana, tra imputato "organo" e "oggetto" di prova, tant'è vero che numerose pronunce si richiamano al *dictum* enunciato dalla Corte Suprema nel risalente caso *Holt c. Stati Uniti*[102], ove si affermò, per la prima volta, che il V Emendamento dev'essere interpretato come un divieto di utilizzo della costrizione per estorcere dichiarazioni dall'imputato, ma non anche per rilevare elementi di prova dal suo "corpo".

A tale orientamento, però, si è vivacemente contrapposta una condivisibile esegesi giurisprudenziale[103] che, per contro, sostiene l'incoercibilità del diniego di "consegnare" i "codici di sblocco 2.0" dei propri dispositivi, facendo leva su quella che è stata plasticamente definita *testimonial biometric doctrine*[104]. Dopo aver sottolineato la profonda differenza che intercorre tra il rilevamento forzoso delle impronte digitali a fini di mero riconoscimento (attività pacificamente non coperta dal V Emendamento[105]) e lo svolgimento della medesima operazione per accedere a un *database* contente informazioni riservate, i giudici sono giunti ad attribuire natura "comunicativa" alla *compulson biometric disclousure*. L'atto in questione – si sostiene – rappresenta una "dichiarazione implicita" del fatto che il sospetto possiede il controllo del dispositivo. Da quest'angolo di visuale, quindi, la "costrizione biometrica" assume i caratteri di un comportamento autoincriminante, poiché l'indagato, pur contro la propria volontà, consente agli inquirenti di apprendere i contenuti del proprio dispositivo e, dunque, potenziali prove a carico.

Il ragionamento, a ben considerare, non si discosta poi molto da quello richiamato da una parte della dottrina americana – e accolto anche sul versante nazionale – con riguardo all'impiego dei *thermal imagers*, cioè mezzi di ricerca della prova utilizzati per individuare le coltivazioni di marijuana *indoor*. In quel contesto, lo si ricorderà, è stato sostenuto che il campo di applicazione del *privilege* dovesse estendersi fino a ricomprendere quelle attività inquirenti che sfruttano le "risposte fisiologiche" dell'indagato, siano esse o meno volontarie. Per tale ragione, si è concluso nel senso che le informazioni così ottenute «costituiscono l'equivalente di una dichiarazione *contra se*, a rendere la quale un soggetto non può essere costretto secondo la protezione accordatagli […] dal V Emendamento»[106].

---

la quale «*there is no dispute that passwords are testimonial in nature and requir defendants to recall the passwords from their own minds; however, biometrics are very different because placing a finger on a biometric sensor is purely a physical act*»; Z.E. JACOBSON, *Face Off: Overcoming the Fifth Amendment Conflict Between Cybersecurity and Self-Incrimination*, in *Journal of Law and Health*, 2023, p. 192.

[101] *Commonwealth c. Baust*, 89 Va. Cir. 267, 271 (2014), trad. nostra.

[102] *Holt c. Stati Uniti*, 218 U.S. 245 (1910).

[103] Cfr., ad es., *Search of a Residence in Oakland*, 354 F. Supp. 3d 1010, 1015 (N.D. Cal. 2019); *Stati Uniti c. Wright*, 431 F. Supp. 3d 1175, 1181 (D. Nev. 2020).

[104] H. METZ, *"Your Device is Disabled": How and Why Compulsion of Biometrics to Unlock Devices Should be Protected by the Fifth Amendament Privilege*, in *Valparaiso University Law Review*, 2019, p. 427 ss.

[105] *Stati Uniti c. Wade*, 388 U.S. 218, 223, 87 S.Ct. 1926.

[106] Testualmente, M. MIRAGLIA, *Garanzie costituzionali nel processo penale statunitense. Tendenze e riflessioni*, Torino, 2008, p. 27, alla quale si rinvia per una più ampia riflessione sul tema.

4.2 La valutazione *contra se* del contegno non collaborativo dell'indagato: la negazione giurisprudenziale del "diritto di esercitare i diritti"

Un'ulteriore notazione appare, a questo punto, necessaria.

L'esercizio di un diritto riconosciuto dall'ordinamento, perdipiù se avente rango costituzionale, non può produrre alcuna conseguenza pregiudizievole in capo al suo titolare; diversamente argomentando, quell'attribuzione si rivelerebbe meramente illusoria, giacché condizionare un diritto a conseguenze negative, equivale, sostanzialmente, a negarlo. Il principio appena enunciato ha carattere universale, ma trova feconda applicazione anche con riguardo al tema in esame. In effetti, se il diritto al silenzio, pur non godendo di espresso riconoscimento costituzionale, rappresenta un «corollario essenziale dell'inviolabilità del diritto di difesa»[107], il diniego manifestato dall'indagato a fronte della richiesta dell'autorità di fornire i codici di accesso ai dispositivi elettronici e alle pagine *social* non può assumere alcuna valenza probatoria.

Questa basilare regola di civiltà giuridica, però, non pare essere stata interiorizzata a pieno dalla giurisprudenza di legittimità italiana che, per contro, ha recentemente manifestato un orientamento incline a disconoscere il valore rappresentato dal *nemo tenetur*. Il riferimento, più in particolare, è a due pronunce adottate dalla II Sezione della Suprema corte nelle quali è stata indirettamente riconosciuta una portata *contra se* al rifiuto del ricorrente di fornire i codici di sblocco.

Con riguardo alla prima[108], i giudici hanno desunto la sussistenza del pericolo «concreto e attuale» di inquinamento probatorio *ex* art. 274, comma 1, lett. a), c.p.p. dal rifiuto del ricorrente di svelare le *password* di accesso ai propri dispostivi. Ad avviso della Corte, il pieno riconoscimento della libertà di circolazione in capo al ricorrente avrebbe potuto aumentare il rischio che l'indagato cancellasse, da remoto, i dati contenuti nel *device* oggetto di sequestro. Ora, nessuno dubita dell'esistenza di un tale rischio – come dimostra una recente pronuncia in tema di sottrazione o danneggiamento di cose sottoposte a sequestro (art. 334 c.p.)[109] –, ma ciò, a ben vedere, non può giustificare il ricorso a interpretazioni apertamente elusive del dettato normativo. Il codice di rito, sul punto, è oltremodo chiaro: il *periculum* che giustifica l'emissione di una misura cautelare non può «essere individuato nel rifiuto della persona sottoposta alle indagini o dell'imputato di rendere dichiarazioni».

Sennonché, lo stesso *modus pensandi* è stato adottato in un successivo arresto del 2023 con il quale i giudici di terza istanza, dopo aver riconosciuto che «la mancata collaborazione dell'indagato nel fornire le chiavi di accesso è un comportamento sicuramente inquadrabile come esercizio del […] diritto al silenzio», hanno qualificato tale condotta alla stregua di un *quid* idoneo a influire sulla «valutazione della legittimità della protrazione» del sequestro probatorio di un dispositivo elettronico[110]. Secondo la Corte, la "ragionevole durata del

[107] Corte cost., ord., 24 giugno 2004, n. 202.

[108] Cass. pen., Sez. II, 26 febbraio 2021, n. 7568, in *Dir. Internet*, 12 marzo 2021.

[109] Cass. pen., Sez. V, 21 ottobre 2022, n. 4343, secondo la quale «integra il delitto di cui all'art. 334 cod. pen. la condotta del proprietario di uno "*smartphone*" sottoposto a sequestro probatorio che, accedendo da remoto al dispositivo, cancelli tutti i dati informatici in esso presenti, trattandosi di reato a forma libera suscettibile di essere commesso anche con modalità telematiche».

[110] Cass. pen., Sez. II, 23 marzo 2023, n. 17604.

vincolo" – imposta, come si è visto, alla luce del principio di proporzionalità – è strettamente dipendente dalle eventuali difficoltà tecniche incontrate dagli esperti al momento dell'estrazione dei dati; difficoltà che – e questo è il passaggio fondamentale dell'intero snodo argomentativo – risultano «accresciute dalla indisponibilità delle chiavi di accesso». Il messaggio che traspare dalla lettura della sentenza è difficilmente equivocabile: la mancata comunicazione delle *password* da parte dell'indagato incide sulla estensione temporale del vincolo e, di conseguenza, il ritardo nel dissequestro/restituzione del *device* può essere imputato solo a quest'ultimo.

Nihil sub sole novum, si dirà. E, in effetti, il retropensiero culturale sotteso a una simile impostazione si è manifestato, per lungo tempo, con riguardo all'istituto della riparazione per ingiusta detenzione[111]. Il quadro, però, è decisamente mutato a seguito dell'approvazione del d.lgs. 8 novembre 2021, n. 188, con il quale il legislatore è intervenuto al fine di adeguare la normativa nazionale alle disposizioni contenute nella Direttiva 2016/343/UE. Allo stato attuale, il nuovo art. 314, comma 1, c.p.p., dopo aver delineato i requisiti della cd. ingiustizia sostanziale, stabilisce che «l'esercizio da parte dell'imputato della facoltà di cui all'articolo 64, comma 3, lettera b), non incide sul diritto alla riparazione». Il *novum* normativo, in questo caso, ha sortito l'effetto sperato e la giurisprudenza sembra essersi assestata su un'interpretazione più rispettosa dei canoni costituzionali: «il silenzio serbato dall'indagato […] nell'esercizio della facoltà difensiva prevista dall'art. 64, comma 3, lett. b), cod. proc. pen., non rileva quale comportamento ostativo alla insorgenza del diritto alla riparazione»[112].

Alla luce di tali considerazioni, non sembra peregrino invocare, pure nel contesto della crittografia digitale, un intervento legislativo che stronchi sul nascere le derive interpretative delle quali si è dato conto. Non è superfluo ribadire, ancora una volta, che l'esercizio del diritto al silenzio, garantito dalla Costituzione, non può avere alcuna conseguenza pregiudizievole in capo al suo titolare, con ciò dovendosi intendere sia un divieto di valutazione probatoria a sfavore di chi tace, sia, più in generale, un obbligo per il giudice e il pubblico ministero di considerare quella condotta alla stregua di un «dato procedimentale neutro»[113].

---

[111] La giurisprudenza, infatti, nel tentare di conciliare l'esercizio del diritto al silenzio riconosciuto all'indagato con la incidenza che tale comportamento può assumere in termini di condotta gravemente imprudente o negligente, ha affermato a più riprese che l'avvalersi della facoltà di non rispondere assumere rilievo ai fini dell'accertamento della sussistenza della condizione ostativa del dolo o della colpa grave, «poiché è onere dell'interessato apportare immediati contributi o riferire circostanze che avrebbero indotto l'Autorità Giudiziaria ad attribuire un diverso significato agli elementi posti a fondamento del provvedimento cautelare» (da ultimo, Cass. pen., Sez. III, 10 giugno 2020, n. 19063).

[112] Così, a seguito dell'entrata in vigore del d.lgs. 188/2021, Cass. pen., Sez. IV, 8 febbraio 2022, n. 8616. Conforme, Cass. pen., Sez. IV, 12 aprile 2022, n. 19621. È rimasto immutato, al contrario, l'orientamento della Suprema corte con riguardo alla rilevanza del mendacio tenuto dall'indagato in sede di interrogatorio. In questo caso – si afferma – «la falsa prospettazione di situazioni, fatti o comportamenti, anche a seguito della modifica dell'art. 314 cod. proc. pen., non è condotta assimilabile al silenzio serbato nell'esercizio della facoltà difensiva prevista dall'art. 64, comma 3, lett. b) cod. proc. pen». Di talché, l'esercizio della facoltà di mentire in sede di interrogatorio, ove causalmente rilevante ai fini dell'intervento dell'autorità, è «suscettibile di incidere sull'accertamento dell'eventuale dolo o colpa grave ostativi al riconoscimento del diritto alla riparazione, in quanto condotta volontaria fortemente equivoca e ambigua» (cfr. Cass. pen., Sez. IV, 20 gennaio 2022, n. 3755; Cass. pen., Sez. IV, 30 giugno 2022, n. 30056).

[113] P. MOSCARINI, *Il silenzio dell'imputato sul fatto proprio secondo la Corte di Strasburgo e nell'esperienza italiana*, in *Riv. it. dir. proc. pen.*, 2006, p. 632.

4.3 L'estensione del "*social network privilege*" alla persona non sottoposta a indagini

Quanto alla latitudine del *nemo tenetur se ipsum accusare*, sembra potersi sostenere la possibilità di dilatare l'ambito di copertura della garanzia anche con riguardo alla persona non sottoposta a un'indagine penale[114], pur con alcune, doverose, precisazioni.

È ben noto che sul soggetto chiamato a rendere dichiarazioni dinnanzi all'autorità inquirente nel corso della fase preliminare (e dibattimentale) gravi un generale obbligo di collaborazione, cioè, un vero e proprio dovere di concorrere all'accertamento del fatto oggetto del processo; un postulato, questo, che si ricava direttamente dal più ampio dovere inderogabile di solidarietà sociale sancito all'art. 2 Cost.[115]. Questo principio generale, però, incontra un limite nel disposto degli artt. 63 e 198 c.p.p., nella parte in cui si riconosce il privilegio contro l'autoincriminazione in capo alla persona non sottoposta a indagine chiamata a deporre dinnanzi all'autorità. Il *nemo tenetur detegere turpitudinem suam*, infatti, implica che nessuno, neppure il testimone, possa essere obbligato a rendere affermazioni dalle quali potrebbero emergere indizi di reità a suo carico.

L'estensione della garanzia a favore di coloro che non sono formalmente sottoposti a un procedimento penale è stata, di recente, nuovamente avallata dalla Corte costituzionale[116] che, sulla scorta di alcune considerazioni offerte dai giudici del Kirchberg[117], ha esteso l'ambito di applicazione del diritto al silenzio alla richiesta di fornire informazioni a un'autorità ispettiva nel quadro di un'attività di vigilanza tanto in un «momento successivo alla contestazione formale» dell'illecito, quanto – ed è questo il passaggio della pronuncia che più interessa – nel caso in cui l'esame sia «funzionale alla scoperta di illeciti e alla individuazione dei responsabili». In questa prospettiva, dunque, la facoltà di non autoincriminarsi non si limita a "coprire" solamente le mere "dichiarazioni" di natura confessoria, ma assume una portata particolarmente estesa, «comprendendo il diritto di ogni cittadino di non fornire elementi che possano portare alla sua incriminazione, intesa come apertura di un procedimento [penale] a suo carico»[118]. Da questo punto di vista, perciò, la consegna delle chiavi di accesso ai propri dispositivi potrebbe doversi considerare alla stregua di una condotta potenzialmente autoincriminante.

Vi è un aspetto, tuttavia, che sembra allontanare l'ipotesi in esame dal raggio di operatività degli artt. 63 e 198 c.p.p.

Innanzitutto, come si è visto, le predette disposizioni si riferiscono esclusivamente alle «dichiarazioni» dalle quali potrebbero emergere indizi *contra se*, ma non anche alle "condotte" attive non aventi natura comunicativa, come nel caso della dazione di una

---

[114] In tal senso, v., esplicitamente, L. LUPÁRIA, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, cit., p. 160, per il quale «il diritto a non collaborare spetta non solo alla persona indagata, ma anche a chi rischia di far emergere una sua responsabilità penale attraverso la dazione di codici».

[115] Da ultimo, sulla cd. servitù di giustizia del terzo, v. C. CONTI, *Il corpo dell'imputato come prova: il diritto di non collaborare tra prospettive sovraordinate, suggestioni storiche e polifunzionalità dei dati*, in *Dir. pen. proc.*, 2024, p. 109 ss.

[116] Corte cost., 30 aprile 2021, n. 84, par. 3.6.

[117] CGUE, 2 febbraio 2021, C-481/19, Consob. Cfr., per tutti, G. LASAGNI, *La Corte di giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi (e la Corte costituzionale conferma)*, in *Giur. comm.*, 2021, p. 1179 ss.

[118] O. MAZZA, *Presunzione d'innocenza e diritto di difesa*, in *Dir. pen. proc.*, 2014, p. 1409. L'assunto è ampiamente avallato dalla giurisprudenza europea: cfr. Corte edu, 4 ottobre 2005, *Shannon c. Regno Unito*.

password. Per di più, la sanzione dell'"inutilizzabilità relativa" *ivi* prevista presuppone che gli indizi di reità emergano contestualmente al rilascio del contributo dichiarativo, cosa che non si verifica nell'ipotesi della semplice dazione della *password*.

Ora, pur volendo (legittimamente) estendere in concetto di "dichiarazione" fino a ricomprendervi qualunque comportamento proattivo, non v'è dubbio che l'atto di rivelazione delle credenziali assuma, come detto, un carattere neutro, di talché un'eventuale portata autoincriminante potrebbe emergere solo a seguito del successivo accertamento tecnico-informatico disposto sul *device*.

A fronte di tale quadro, potrebbe forse ipotizzarsi, *de lege ferenda*, una modifica normativa volta a cristallizzare un'ipotesi di "inutilizzabilità soggettivamente relativa"[119] delle informazioni *contra se* emerse dall'analisi del *device*, garantendo, per contro, la spendibilità processuale degli elementi di prova a carico di terzi. Si tratta di una soluzione di compromesso che, allo stato attuale, parrebbe, *prima facie*, in grado di contemperare l'esigenza di tutelare il privilegio contro l'autoincriminazione in capo al terzo e, contestualmente, la necessità di garantire indagini penali davvero efficaci.

Ciò nondimeno, il supposto scenario non sembra comunque del tutto soddisfacente. L'autorità inquirente, dopo aver ottenuto l'accesso al dispositivo, potrebbe utilizzare le informazioni raccolte come spunto investigativo per lo svolgimento di indagini a carico del terzo o financo come vere e proprie *notitie criminis*, privando così il privilegio della sua intrinseca portata garantista.

Al fine di scongiurare tale pericolo, occorre soffermare l'attenzione sulla necessità di predisporre una garanzia a monte, cioè un presidio atto a scongiurare il rischio di un'intrusione arbitraria nella vita privata dei terzi coinvolti. A tale scopo, assume una certa consistenza il disposto dell'art. 19, comma 4, della Convenzione sul *Cybercrime*, a mente del quale gli Stati contraenti devono adottare le misure legislative necessarie per consentire alle proprie autorità nazionali di «ordinare ad ogni soggetto che abbia conoscenza del funzionamento del sistema informatico o delle misure utilizzate per proteggere i dati informatici in esso contenuti, di mettere a disposizione tutte le informazioni ragionevolmente necessarie» per consentire l'accesso a detti sistemi. Dalla lettura della norma emerge, con tutta evidenza, la centralità che va acquisendo il canone di proporzionalità quale "parametro guida" capace di indirizzare e, allo stesso tempo, limitare, l'attività investigativa digitale, ponendosi quale argine alla bulimia acquisitiva propria delle investigazioni tecnologicamente assistite.

Cercando di valorizzare a pieno tale principio[120], la "ragionevole necessità" che giustifica l'intrusione statale nel "domicilio informatico" del terzo potrebbe modellarsi diversamente a seconda del tipo di interesse coinvolto. In alcune circostanze, essa potrebbe legittimare *tout*

[119] Trattasi, come noto, di quella forma di inutilizzabilità che «rende l'atto invalido nei confronti di determinate persone» (C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penal*e, Padova, 2007, p. 29).

[120] Nel paragrafo n. 146 dell'*Explanatory Report to the Convention on Cybercrime*, peraltro, si prevede espressamente che «*the powers and procedures shall "incorporate the principle of proportionality". Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law*».

court la divulgazione della *password* o delle altre misure di sicurezza, salvo, in ogni caso, la previsione di una tutela a valle (si legga, inutilizzabilità). In altre, invece, una tale ingerenza potrebbe non apparire proporzionata rispetto all'obiettivo perseguito, cosicché, in queste ipotesi, la divulgazione delle «informazioni necessarie» potrebbe consistere nella mera consegna del materiale probatorio concretamente richiesto dall'autorità inquirente. La logica della proporzionalità, in altri termini, dovrebbe consentire di modulare il grado di esigibilità della collaborazione del terzo a seconda della tipologia di dati richiesti e della gravità del reato per il quale si sta procedendo. Nel solco di quella che la miglior dottrina ha definito una «"tutela progressiva" dei diritti di libertà»[121], del resto, il principio *de quo* impone di individuare limiti ben definiti oltre i quali il potere pubblico non può spingersi, neppure per il perseguimento della legittima finalità di repressione criminale.

Un modello cui fare riferimento potrebbe essere, ancora una volta, quello iberico e, più in particolare, la normativa racchiusa nell'art. 588-*sexies* c) della *Ley de enjuiciamiento criminal*. La disposizione, nel dare attuazione al contenuto dell'art. 19, comma 4 della Convenzione di Budapest, cristallizza un dovere generale di collaborazione con la giustizia, stabilendo che gli inquirenti possono «ordinare a chiunque sia a conoscenza del funzionamento di un sistema informatico o delle misure di protezione dei dati informatici in esso contenuti» di fornire le informazioni necessarie, «*siempre que de ello no derive una carga desproporcionada para el afectado*»[122]. Al di là delle critiche mosse da una parte della dottrina[123], il riferimento a un "onere sproporzionato" per la parte interessata (si legga, il terzo estraneo alle indagini) consente di enucleare quello che potremmo definire un principio di non intrusione nella sfera di riservatezza dei terzi, la cui modulazione si giustifica proprio alla luce del canone di proporzionalità.

5. Accesso occulto e da remoto a informazioni non comunicative mediante *trojan horse*

L'apprensione da parte della polizia giudiziaria di informazioni non aventi natura comunicativa può avvenire, come detto, mediante il sequestro del dispositivo fisico con il

---

[121] R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, p. 1133 ss. e, spec., p. 1151, ove l'A. evidenzia come l'aggettivo «progressiva» intenda segnalare sia l'emersione di nuovi diritti – specialmente a fronte delle nuove capacità intruse proprie dei "mezzi di ricerca della prova 2.0", sia la necessità «di sorvegliare il confine mobile che […] divide l'area dei diritti inviolabili da quella di una loro compressione giustificata dalla necessità di reprimere e/o prevenire attività criminose».

[122] Il secondo comma della disposizione, invero, stabilisce l'inapplicabilità del primo comma «alla persona sottoposta a indagini o procedimenti giudiziari, alle persone esenti dall'obbligo di testimoniare per motivi di parentela e a quelle che, ai sensi dell'art. 416, comma 2, c.p.p., non possono testimoniare in virtù del segreto professionale» (trad. nostra).

[123] La censura riguarda, in particolare, l'impiego dell'espressione «*cualquier persona*», ritenuta eccessivamente generica e potenzialmente in grado di includere anche soggetti estranei alle indagini: «*¿qué perfil tiene esa persona? Al hablarse de un cualquier no se acota la identidad de ese sujeto, ¿se está hablando de un ingeniero informático profesional? O por el contrario ¿se abre la puerta al fichaje de hackers que actúen sin fines éticos e incluso criminales?*» (così, F. BUENO DE MATA, *Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*, in *Diario la Ley*, 19 ottobre 2015, par. 5). Ci si chiede, altresì, se l'obbligo di cooperazione imposto a "chiunque" includa anche il dovere di fornire, su richiesta, all'autorità inquirente, specifici *software* in grado di craccare e sbloccare il dispositivo (cfr., *amplius*, P. MARTIN RIOS, *Digital forensics and criminal process in Spain: evidence gathering in a changing context*, Cizur Menor, 2022, p. 116 ss.).

quale l'indagato (o il terzo) accede al proprio profilo *social*. Si è dato conto, però, delle numerose difficoltà pratico-applicative cui va incontro l'autorità inquirente nell'eseguire tale operazione, come, ad esempio, l'impossibilità di accedere al *device* a causa delle moderne tecnologie di protezione.

Per tale ragione, gli inquirenti hanno individuato una «formidabile scorciatoia»[124] investigativa che consente loro di acquisire in modo occulto le informazioni segrete contenute nello *smartphone* e negli *accounts* dei *social network*. Il riferimento, come può immaginarsi, è al cd. captatore informatico, cioè un *malware* in grado di infettare (anche da remoto) un dispositivo elettronico, al fine di prenderne il controllo e realizzare una molteplicità di operazioni investigative. Il carattere altamente invasivo dello strumento e l'inadeguatezza del dettato normativo hanno stimolato un dibattito dottrinale con riguardo all'ammissibilità del *trojan horse* sia come mezzo di captazione segreta (*rectius*, intercettazione tra presenti, *ex* art. 266, comma 2 e 2-*bis* c.p.p.), sia come vero e proprio "intrusore informatico"[125].

È in quest'ultimo contesto, cioè, nell'ambito delle operazioni di indagine non espressamente regolamentate, che si colloca l'impiego del *virus* nell'ambiente dei *social network*. Si allude, più in particolare, alle funzionalità *keylogger* e *screencast* che, insieme alle altre forme di *online surveillance*, consentono al *malware*, rispettivamente, di acquisire in tempo reale tutto ciò che viene digitato sulla tastiera (compresi i caratteri speciali) o visualizzato sullo schermo di un determinato dispositivo.

Quanto alla prima, la possibilità di attenzionare il soggetto nel momento in cui questo accede al proprio profilo *social* consente alla polizia giudiziaria di apprenderne le credenziali, aggirando (legittimamente?) la garanzia del *nemo tenetur*. L'acquisizione occulta delle credenziali, peraltro, può essere realizzata anche mediante l'impiego del *trojan* con funzionalità *password-logging* che consente di registrare tutte le chiavi di accesso salvate in automatico nel dispositivo[126]. In merito alla seconda, va riconosciuto come la scannerizzazione continuativa di quanto raffigurato sullo schermo del dispositivo attenzionato[127] sia in grado di rivelare tutte le attività digitali svolte in Rete dal bersaglio, comprese, per esempio, quelle volte a inserire o modificare le informazioni non comunicative (ma riservate) nel proprio *account social*.

Alla luce dell'estrema pervasività di tale strumento, non possono che essere condivise le preoccupazioni espresse unanimemente dalla dottrina, specialmente con riguardo alla

---

[124] Così la definiscono C. CONTI – M. TORRE, *Spionaggio digitale nell'ambito dei* social network, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 560.

[125] La letteratura sul tema è oramai vastissima. Si rammentino, per tutti, i lavori monografici di M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, Napoli, 2019; W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Milano, 2021; M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit. Per un'efficace *summa* delle principali questioni sul tappeto, v., per tutti e di recente, M. MIRAGLIA, *Il "*Trojan *(non) di Stato": una disciplina da completare*, in *Proc. pen. giust.*, 2023, p. 1227 ss., alla quale si rinvia per ulteriori e puntuali riferimenti bibliografici.

[126] Su questa specifica funzionalità, v. G. COSTABILE – S. ATERNO, *Le intercettazioni digitali*, in AA.VV., Cyber forensics *e indagini digitali*, cit., p. 352.

[127] In questa circostanza, si è plasticamente osservato come il captatore operi «come se fosse un vero e proprio specchio dello schermo» (così, C. CONTI – M. TORRE, *Spionaggio digitale nell'ambito dei* social network, cit., p. 562).

necessità di un intervento legislativo che disciplini, in maniera chiara, precisa e puntuale, se, come e in base a quali criteri dette attività investigative possono essere legittimamente realizzate[128].

6. L'acquisizione delle comunicazioni scritte e orali scambiate mediante le piattaforme di messaggistica istantanea

Quali strumenti di interazione sociale, le moderne piattaforme digitali di comunicazione possono senz'altro essere annoverate nella categoria dei *social network sites*. *Whatsapp*, *Messanger*, *Telegram*, *Snapchat* e le numerose applicazioni di messaggistica istantanea messe a disposizione da *Instagram* e *LinkedIn*, solo per fare alcuni esempi, hanno assunto via via una portata relazionale[129], tale da renderle in tutto e per tutto annoverabili tra le "reti sociali digitali" del XXI secolo[130].

A tal proposito, non v'è dubbio che le informazioni contenute in queste piattaforme di *instant messaging* abbiano ormai assunto una rilevanza probatoria fondamentale.

Prima di esaminare nel dettaglio i risvolti processuali, però, è necessario dare conto di alcune caratteristiche propriamente tecnico-informatiche di tali strumentazioni. Deve ammettersi, infatti, che per comprendere a pieno le potenzialità – e, di riflesso, i nodi problematici – posti da un nuovo strumento tecnologico, sia necessario conoscere il concreto funzionamento delle strutture e dei meccanismi a esso sottesi. Senza voler giungere a teorizzare la necessità di una vera e propria capacità programmatoria del giurista, l'impostazione qui privilegiata sembra trovare conferma in quelle autorevoli voci dottrinali che suggeriscono la necessità, nel campo oggetto del presente studio, di adottare un approccio che potremmo definire "duale": giuridico e, contestualmente, tecnico-informatico[131]. Se non è revocabile in dubbio, infatti, che né la scienza, né, tantomeno, la tecnologia possono essere dominate dal giurista e che queste ultime devono sottostare alle cadenze procedimentali ed epistemologiche del processo, ciò, a tutto concedere, non esime lo studioso dall'approcciarsi a tali questioni con uno sguardo sempre rivolto al "dato informatico".

In primo luogo, le piattaforme di *real-time conversations* consentono ai propri utenti di comunicare tra loro previo *download* sul proprio *device* (fisso o mobile) di un'applicazione *ad hoc*, cosicché l'interazione può avvenire solo tra coloro che sono iscritti alla piattaforma (*rectius*, titolari di un apposito *account social*).

---

[128] Cfr., per un'esaustiva panoramica, W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, cit., *passim*.

[129] Si pensi, ad esempio, alla nuova funzionalità *community* presente nell'applicazione *Whatsapp* o alla possibilità di creare veri e propri profili di gruppo nel *social network Instagram*.

[130] In questo senso, v. TAR Emilia-Romagna, Sez. I, 19 febbraio 2021, n. 124. In dottrina, esplicitamente, A. AGUSTINOY GUILAYN – J. MONCLÚS RUIZ, *Aspectos Legales de las Redes Sociales*, Madrid, 2021, p. 75.

[131] Questo concetto è stato espresso, in maniera chiara e puntuale, nell'*Intervento* della Prof.ssa Curtotti nel corso del *II° Convegno annuale Penale Diritto e Procedura*, reperibile al sito *https://www.youtube.com/watch?v=Wg-rIinQCVE*. Ne è espressione, altresì, la scelta della Prof.ssa Silvia Signorato di dedicare la prima parte (p. 3-48) della monografia *Le indagini digitali*, cit., a un'approfondita esposizione delle principali questioni tecnologiche legate al tema delle indagini a contenuto informatico («la precomprensione dei profili tecnici rappresenta non di rado una precondizione della comprensione di quelli giuridici», p. 323). Lo stesso concetto è fatto proprio anche da W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, cit., p. 1, nt. 1.

In secondo luogo, queste piattaforme permettono oggi di inviare non solo messaggi di testo, ma anche *file* contenenti fotografie e "note vocali", nonché di condividere financo la propria ubicazione (pure in tempo reale).

In terzo luogo, i fornitori del servizio di messaggistica utilizzano perlopiù protocolli di sicurezza per garantire la cifratura delle informazioni che transitano nella Rete. Dal 2016, ad esempio, *Whatsapp* protegge le comunicazioni degli utenti tramite il protocollo *end-to-end* che garantisce la loro piena segretezza[132]; lo stesso avviene per quanto riguarda la funzionalità "chiamate", anch'essa protetta dalla crittografia VoIP-*Voice over IP* (Voce tramite protocollo *Internet*)[133]. Trattasi, in generale, di tecniche che permettono di "oscurare" il contenuto di una chiamata o di un messaggio rendendolo "inaccessibile" a tutti – e, dunque, anche al *Social network provider* che gestisce il servizio[134] –, fuorché al mittente e al suo destinatario. A seguito dell'invio di un messaggio, infatti, questo viene codificato per poi essere decodificato soltanto quando giunge nel dispositivo del ricevente. Lungo il tragitto che separa i *devices*, pertanto, l'informazione è protetta da un "lucchetto crittografico", le cui chiavi sono nella esclusiva disponibilità del destinatario.

Infine, mette conto osservare come queste nuove piattaforme digitali abbiano definitivamente sdoganato le cd. comunicazioni asincrone, sviluppatesi con l'avvento dei primi servizi di *web-e-mail*. Con tale espressione, si allude a una modalità differita di trasmissione dei dati, nel senso che lo scambio di informazioni non richiede più il collegamento contemporaneo degli interlocutori alla Rete; ragion per cui i messaggi possono essere scritti e inviati in un tempo *x* e letti dal destinatario in un tempo *y*. In questi casi, detto altrimenti, non vi è corrispondenza tra il momento in cui il flusso comunicativo fuoriesce dalla psiche del mittente e quello in cui giunge a conoscenza del ricevente.

Alla luce dei connotati tecnici appena descritti, occorre chiedersi, *in primis*, se le comunicazioni asincrone di cui si va discutendo siano o meno ricomprese nel campo di applicazione dell'art. 15 Cost. In caso di risposta affermativa, poi, è necessario valutare se e come esse possano essere apprese dalle autorità inquirenti.

Sul primo versante, come si è già osservato[135], l'esegesi letterale della disposizione costituzionale consente di affermare che l'oggetto della tutela è accordato sia alla «corrispondenza», sia a «ogni altra forma di comunicazione». Proprio l'impiego di una formula tanto ampia e generica – da risultare, a tratti, di difficile intellegibilità[136] – ha indotto

---

[132] Nella pagina informativa sui servizi di *Whatsapp* può leggersi quanto segue: «la crittografia *end-to-end* garantisce che solo tu e la persona con cui stai comunicando possiate leggere o ascoltare i contenuti inviati. Nessuno, nemmeno *WhatsApp*, potrà accedere ai contenuti delle tue comunicazioni».

[133] C. PARODI, VoIP, Skype *e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?*, in *Dir. pen. proc.*, 2008, p. 1310, il quale sottolinea come «*VoIP - Voice over IP* (Voce tramite protocollo *Internet*) – è una tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione *Internet* o un'altra rete dedicata che utilizza il protocollo IP, anziché passare attraverso la rete telefonica tradizionale (PSTN)». Cfr., per un'accurata descrizione, M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., p. 161, nt. 1.

[134] Ciò significa che, ad esempio, se la l'autorità investigativa chiedesse a *WhatsApp* i dati delle conversazioni fra due soggetti, questo non sarebbe in grado di fornirglieli.

[135] Cfr. Parte II, Cap. II.

[136] Come osserva L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. pen. giust.*, 2020, p. 296, «non sempre è agevole riconoscere ed

la miglior dottrina a proporre un'interpretazione particolarmente estesa di tale concetto, fino a ricomprendervi qualunque forma di scambio informativo interpersonale, a prescindere dal tipo di contenuto tramesso e dalla modalità adoperata[137]. Ciò che rileva, in buona sostanza, è la presenza di un *corpus* e un *animus comunicandi*, cioè di un pensiero oggettivamente percepibile che si intende veicolare a un soggetto determinato.

Un approccio di questo tipo, ancorché adottato in un'epoca nella quale la comunicazione per eccellenza era quella cartaceo-epistolare, si rivela ancora oggi attuale. Difatti, se il contenuto del precetto è volto a tutelare, al contempo, la libertà e la segretezza di qualunque «trasmissione intersoggettiva del pensiero umano»[138], non vi sono ragioni per escludere dal novero delle comunicazioni coperte dalla garanzia costituzionale anche quelle realizzate per il tramite dei moderni servizi di *instant messaging*[139]. Del resto, la stessa Corte delle Leggi ha recentemente riconosciuto che il diritto di cui all'art. 15 Cost. «comprende tanto la "corrispondenza" quanto le "altre forme di comunicazione", incluse quelle telefoniche, elettroniche, informatiche, tra presenti o effettuate con gli altri mezzi resi disponibili dallo sviluppo della tecnologia»[140]. In questa prospettiva, pure le nuove forme di comunicazione non verbali adottate dai *millennials* (le cd. *emoticon*) rientrerebbero a pieno titolo nella tutela approntata dalla norma costituzionale. Si è già sottolineato[141], infatti, che nell'ambito dei *social network* è possibile distinguere due tipologie di comportamenti comunicativo-relazionali: da un lato, i cd. *pure speeches* e, dall'altro, per l'appunto, le cd. *symbolic expressions*, ovverosia quelle forme di divulgazione del pensiero che prescindono dal ricorso al sistema alfanumerico tradizionale[142].

Una volta ricondotte le comunicazioni scambiate attraverso le nuove piattaforme di *real-time conversations* nel campo di applicazione dell'art. 15 Cost., se ne ricava, sul piano delle garanzie processuali, la necessità che la compromissione della segretezza possa essere ammessa solo in presenza di due condizioni: riserva di legge e riserva di giurisdizione. Ciò nondimeno, appare forse eccessivamente *tranchant* voler ricondurre qualunque

---

inquadrare ciò che costituisca davvero "comunicazione" da ciò che ne esuli. La possibilità di invocare la protezione assicurata da tale articolo corre sul filo di questa difficile distinzione».

[137] P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, p. 164. Tra i processualisti, v., per tutti, F. CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, p. 43.

[138] F. CAPRIOLI, *Colloqui riservati e prova penale*, cit., p. 48.

[139] Anche secondo A. DIDDI, *L'inviolabilità della segretezza delle comunicazioni*, in F.R. Dinacci (a cura di), *Processo penale e costituzion*e, Milano, 2010, p. 269, la circostanza che l'art. 15 Cost. non operi alcun riferimento al mezzo utilizzato per comunicare, induce a ritenere che la disposizione costituzionale sia volta a tutelare anche «le nuove forme di comunicazione, come i messaggi di posta elettronica, le comunicazioni scambiate in *chat* e le videoconferenze».

[140] Corte cost., 24 gennaio 2017, n. 20, par. 3.3. Nella medesima prospettiva, v. A. VALASTRO, *Libertà di comunicazione e nuove tecnologie. Inquadramento costituzionale e prospettive di tutela delle nuove forme di comunicazione interpersonale*, Milano, 2001, p. 117.

[141] Cfr. Parte I, Cap. II, par. 3.

[142] Del resto, la dottrina più accreditata ha agevolmente ricondotto nel precetto costituzionale tutti quei messaggi a contenuto emotivo, le espressioni scherzose e le comunicazioni gestuali (F. CAPRIOLI, *Colloqui riservati e prova penale*, cit., p. 178). Anche C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., p. 221, sostiene la natura *stricto sensu* comunicativa di quei «comportamenti finalizzati a trasmettere ad altra persona un contenuto di pensiero con la parola, i simboli grafici, i gesti, le espressioni fisiognomiche o qualunque atteggiamento idoneo a comunicare e finalizzato a farlo». Critica, invece, la posizione manifestata da A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, p. 1201.

comunicazione intercorsa nelle *chat* di *Whatsapp*, *Instagram* e le altre applicazioni di messaggistica sotto la copertura costituzionale dell'art. 15 Cost.

A tal proposito, occorre tentare di operare alcune distinzioni[143].

A) Innanzitutto, non sembra potersi ricomprendere nel concetto di "comunicazione" la condotta del soggetto che si limita a digitare sulla tastiera del proprio dispositivo un messaggio scritto o a registrare un messaggio vocale (*corpus comunicandi*) in assenza di una espressa *voluntas comunicandi*, cioè in mancanza di una manifesta «intenzione di farlo pervenire ad un altro soggetto»[144]. Al pari delle *email* "parcheggiate" nella cartella "bozze" o di un qualunque scritto epistolare destinato a rimanere alla stregua di una semplice nota di carattere personale, l'assenza di una volontà comunicativa e di un flusso materiale di dati rende, di riflesso, inapplicabile la disciplina delle intercettazioni[145].

[143] Un esempio emblematico delle numerose complessità legate al tema dell'acquisizione delle "informazioni segrete" contenute nei moderni strumenti di comunicazione riguarda la captazione delle conversazioni scambiate mediante piattaforme criptate, i cd. criptofonini. Trattasi, in strema sintesi, di *smartphones* modificati all'origine e progettati per garantire uno scambio di flussi di informazioni sicuro e protetto. Proprio questa caratteristica li ha resi appetibili per le associazioni criminali transnazionali, le quali utilizzano detti apparati per comunicare in via riservata (si pensi a *EncroChat* o a Sky ECC). Una delle questioni di maggior interesse che si è posta a livello nazionale (e non solo) riguarda la natura giuridica da riconoscersi agli atti di indagine compiuti in Italia consistenti nell'apprensione, mediante OEI, delle comunicazioni trasmesse dalle autorità francesi, già acquisite e decriptate nel corso di un procedimento penale straniero. Sul punto, si sono andati delineando plurimi orientamenti interpretativi. Secondo una prima esegesi, le comunicazioni effettuate tramite criptofonini, i quanto rinvenibili in *server* situati all'estero, possono essere acquisite mediante OEI e legittimamente utilizzate in Italia alla stregua di documenti informatici *ex* artt. 234 o 234-*bis* c.p.p. (cfr., ad es., Cass. pen., Sez. III, 19 ottobre 2023, n. 47201; Cass. pen., Sez. IV, 28 marzo 2023, n. 19623). Ad opposta conclusione, giunge, invece, altra giurisprudenza di legittimità, secondo la quale la fattispecie applicabile nel caso in esame è quella prevista all'art. 254-*bis* c.p.p. in tema di sequestro (Cass. pen. VI, 26 ottobre 2023, n. 44154). In dottrina, invero, si è prospettata un ulteriore ermeneusi: quando la comunicazione è ancora in corso, l'acquisizione dei dati dovrebbe avvenire utilizzando la forma dell'ordine europeo di intercettazione; per contro, si dovrebbe disporre un ordine europeo di sequestro qualora si tratti di comunicazioni già inviate, lette e conservate in determinati dispositivi informatici o *server* (cfr. M. DANIELE, *Ordine europeo di indagine penale e comunicazioni criptate: il caso* Sky ECC/Encrochat *in attesa delle Sezioni Unite*, in *Sist. pen.*, 11 dicembre 2023, par. 5). Come prevedibile, il variegato panorama interpretativo ha reso necessario l'intervento delle Sezioni Unite, sollecitate da due ordinanze di rimessione (Cass. pen., Sez. III, ord., 3 novembre 2023, n. 47798; Cass. pen., Sez. VI, ord., 15 gennaio 2024, n. 2329). Con l'informazione provvisoria pubblicata in data 29 febbraio 2024, il Supremo Consesso, con due distinte decisioni, ha stabilito che: a) il trasferimento all'autorità giudiziaria italiana, in esecuzione di ordine europeo di indagine, del contenuto di comunicazioni effettuate attraverso criptofonini e già acquisite e decrittate dall'autorità giudiziaria estera in un proprio procedimento penale, «rientra nell'acquisizione di atti di un procedimento penale che, a seconda della loro natura, trova alternativamente il suo fondamento negli artt. 78 disp. att. c.p.p., 238, 270 c.p.p. e, in quanto tale, rispetta l'art. 6 della Direttiva 2014/41/UE»; b) detto trasferimento non deve essere oggetto di verifica giurisdizionale preventiva della sua legittimità, nello Stato di emissione dell'ordine europeo di indagine, giacché è ricompreso «nei poteri del pubblico ministero quello di acquisizione di atti di altro procedimento penale»; c) l'autorità giurisdizionale dello Stato di emissione dell'ordine europeo di indagine deve verificare il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo. In attesa di conoscere le motivazioni delle pronunce, un dato pare indubitabile: a prescindere dalla/e modalità di acquisizione che si intendano prediligere, alla difesa deve essere attribuita la facoltà di verificare il modo in cui l'autorità straniera ha estrapolato i dati trasfusi nella comunicazione trasmessa all'autorità italiana, onde poter saggiare l'eventuale presenza di alterazioni (pur involontarie) o di manipolazioni dei sistemi informatici. Solo in questo modo, a ben vedere, può essere garantito l'esercizio effettivo del diritto di difesa.

[144] P. BARILE – E. CHELI, voce *Corrispondenza (libertà di)*, in *Enc. dir.*, 1962, p. 745.

[145] Cfr., proprio con riguardo all'ipotesi della "posta elettronica non ancora inviata", Cass. pen., Sez. IV, 28 giugno 2016, n. 40903.

A diverse conclusioni rispetto a quelle qui ipotizzate, però, sembra giungere la giurisprudenza di legittimità. In una recente pronuncia, infatti, la Suprema Corte ha affermato che la semplice visualizzazione di un *file Excel* sullo schermo di un *personal computer*, «pur non costituendo una "comunicazione" in senso stretto, costituisce certamente, invece, un comportamento cd. comunicativo, del quale è ammessa la captazione [mediante l'impiego del *trojan horse*]»[146]. Il costrutto argomentativo alla base della sentenza poggia su un (assai) discutibile interpretazione della locuzione "flusso comunicativo di dati informatici", alla quale viene ricondotto anche il mero transito unidirezionale di dati confinati all'interno dei circuiti di un *personal computer*.

L'esegesi in parola si presta a un duplice ordine di censure[147].

In primo luogo, è lecito dubitare della riconducibilità delle operazioni in esame (*rectius*, la visualizzazione di un file sullo schermo di un *device* o la semplice composizione di una parola sulla tastiera) nel concetto di "comunicazione": esso, lo si è detto, postula un dato informativo caratterizzato da una «specifica direzionalità verso il destinatario»[148]. In secondo luogo, l'impostazione adottata dalla pronuncia in esame appare sconfessata da un più risalente (e condivisibile) orientamento della Suprema Corte, stando al quale l'apprensione di dati già presenti e memorizzati nell'*hard disk* di un dispositivo elettronico avrebbe ad oggetto non tanto un flusso di comunicazioni – che, in quanto tale, presuppone «un dialogo con altri soggetti» –, bensì una «relazione operativa tra microprocessore e video del sistema elettronico»[149]. Di conseguenza, il termine "flusso di comunicazioni" – seguendo questa linea esegetica – dovrebbe essere ricondotto esclusivamente a uno scambio di *bit* «tramite la connessione tra *computer* [diversi tra loro]»[150].

Differente rispetto all'ipotesi ora esaminata è, però, il caso in cui più utenti accedano, in momenti diversi, al medesimo *account social* in modo da scambiarsi messaggi concernenti, ad esempio, la commissione di attività criminose. Il problema, come noto, si è posto inizialmente con riguardo alle comunicazioni di posta elettronica non spedite e salvate in modalità *stand by*, rispetto alle quali la giurisprudenza di legittimità ha escluso l'applicazione della disciplina prevista all'art. 266-*bis* c.p.p., poiché, in tali evenienze, non si verrebbe a configurare alcun flusso comunicativo suscettibile di essere captato[151].

L'assunto genera più di qualche perplessità. E, infatti, la dottrina più accorta[152] ha sottolineato come, nonostante la mancata spedizione della *e-mail*, possa comunque profilarsi

---

[146] Cass. pen., Sez. I, 7ottobre 2021, n. 3591.

[147] In termini critici rispetto alla pronuncia in parola, v. A. PROCACCINO, *Piccoli equivoci senza importanza: tra intercettazioni di flussi informatici, perquisizioni e prove atipiche*, in *Cass. pen.*, 2022, p. 3120; M. MIRAGLIA, *Il "*Trojan *(non) di Stato"*, cit., p. 1239, per la quale la corte avrebbe adottato «un atteggiament[o] opportunistic[o] per salvare gli elementi raccolti, la prova atipica, ma anche mezzi di ricerca della prova tipici, con forzature di non poco conto».

[148] Efficacemente, E.M. MANCUSO, *L'acquisizione di contenuti* e-mail, in A. Scalfati (a cura di), *Le indagini atipiche*, cit., p. 514.

[149] Cass. pen, Sez. 14 ottobre 2009, n. 16556.

[150] Cass. pen, Sez. 14 ottobre 2009, n. 16556, cit.

[151] Cass. pen., Sez. IV, 30 settembre 2016, n. 40903.

[152] Cfr., ad es., L. GIORDANO, *Dopo le sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. pen. cont.*, 2017, 3, p. 190; M. TORRE, *Il captatore informatico*, cit., p. 33.

uno scambio informativo tra più soggetti in grado di generare un flusso di dati captabile *ex* art. 266-*bis* c.p.p. In questa ipotesi, del resto, non si realizza forse un atto di natura comunicativa tra due utenti mediante un comportamento (la scrittura del messaggio e i successivi accessi allo spazio virtuale che lo contiene) finalizzato a trasmettere volontariamente e consapevolmente un contenuto di pensiero (*animus comunicandi*)?

B) Diverso è il caso in cui l'organo d'accusa intenda apprendere il contenuto di una conversazione (messaggi di testo, vocali o chiamate) nel momento in cui questa avviene, cioè, quando è in essere un vero e proprio flusso comunicativo. Nessun dubbio che, in tale evenienza, l'acquisizione debba avvenire nel rispetto dei crismi fissati all'art. 266-*bis* c.p.p. (o 266 c.p.p., a seconda dell'interpretazione che si intenda prediligere[153]) che, come noto, disciplina la captazione informatica o telematica di un atto comunicativo mediante strumenti tecnici idonei da parte di un soggetto esterno rispetto ai protagonisti del colloquio. Nell'ipotesi in esame, inoltre, vi è per certo una contestualità tra la comunicazione e l'atto acquisitivo realizzato dall'autorità inquirente, giacché l'apprensione avviene nell'arco di tempo che intercorre tra l'invio del messaggio da parte del "dispositivo generatore" e la ricezione del medesimo ad opera del "dispositivo recettore"[154].

Come si è detto, però, le comunicazioni scambiate tramite le *App* di *social network* non possono essere intercettate con le tradizionali forme di captazione, giacché esse non consentono di analizzare i dati cifrati, né di identificare l'apparato utilizzato per lo scambio di informazioni. Per di più, la contestualità tra l'invio del messaggio e la ricezione (*rectius*, la presa in carico) da parte del dispositivo ricevente, caratteristica propria di tutte le *chat* di *instant messaging*, rende complesso eseguire una captazione del flusso "in tempo reale"[155]. Di queste difficoltà è pienamente consapevole anche il Consiglio europeo che, in una recente Proposta di Risoluzione[156], ha sottolineato come la crittografia rappresenti, nell'attuale realtà digitale, un mezzo necessario per proteggere i diritti fondamentali e la sicurezza dei governi, delle industrie e dei singoli cittadini. Allo stesso tempo, però, il documento prende atto della necessità di introdurre nuove regole (e, con esse, implementare nuove strumentazioni

[153] Vi è un accesso dibattito in merito all'individuazione della normativa di riferimento per eseguire le captazioni di flussi comunicativi in forma digitalizzata. Una parte della dottrina, all'indomani dell'entrata in vigore dell'art. 266-*bis* ad opera della l. 23 dicembre 1993, n. 547, aveva sottolineato l'inutilità e la dannosità di una norma siffatta, posto che le captazioni informatiche o telematiche ben avrebbero potuto essere ricondotte nel campo di applicazione dell'art. 266 c.p.p. e, più in particolare, nel concetto di «altre forme di comunicazione» (per questa opinione, v. A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, p. 12 s. Nello stesso senso, anche con riguardo alle chiamate *VoIP*, L. MARAFIOTI, Digital evidence *e processo penale*, cit., p. 4509 ss.). Altri commentatori, per converso, riconducono l'ipotesi *de qua* nel novero dell'art. 266-*bis* c.p.p., valorizzando la peculiarità delle chiamate *VoIP* rispetto alle telefonate tradizionali (è la tesi sostenuta, ad es., da G. VACIAGO, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012, p. 70 ss.).

[154] Con riguardo al tema delle *chat pin-to-pin*, la Corte di cassazione ha affermato, senza riserve, che la captazione delle informazioni trasmesse via *chat* rientra nel campo di applicazione dell'art. 266-*bis* c.p.p. (Cass. pen., Sez. III, 10 novembre 2015, Guarnera).

[155] Lo sottolinea, da ultimo, pure M. PITTIRUTI, *L'impego processuale dei messaggi inviati mediante l'applicazione* Telegram *tra "scorciatoie" probatorie e massime di esperienza*, in *Dir. Internet*, 2020, p. 317.

[156] CONSIGLIO EUROPEO, *Risoluzione del Consiglio sulla crittografia. La sicurezza attraverso la crittografia e nonostante la crittografia*, 24 novembre 2020.

tecnologiche) affinché sia consentito alle autorità inquirenti e di *law enforcement*, specialmente sul terreno della giustizia penale, l'accesso ai dati scambiati mediante applicazioni protette da sistemi E2EE.

La risposta tecnologica – prima ancora che giuridica – elaborata dai tecnici per far fronte a tali difficoltà consiste nell'impiego delle cd. intercettazioni attive, ovverosia mediante l'uso del captatore informatico[157]. Grazie alla funzionalità *call-logging*, gli inquirenti sono oggi in grado di attivare da remoto il microfono del dispositivo utilizzato per la comunicazione, al fine di intercettare tutte le conversazioni, nonché registrare tutte le sessioni delle *chat* create dall'utente (*chat-logging*).

A fronte dell'evoluzione tecnologica e dei nuovi sistemi di protezione cibernetica, dunque, l'autorità inquirente, nell'ipotesi in esame, non sembra poter rinunciare alle potenzialità captative del *virus* di Stato[158]. Occorre fare i conti con la realtà: una privazione *tout court* di dette strumentazioni si risolverebbe in un'intollerabile menomazione del principio di repressione criminale che, trovando pieno riconoscimento nella Carta Fondamentale, appare funzionale a tutelare il più generale bisogno di sicurezza individuale e collettivo[159]. Il cuore della questione, perciò, non riguarda l'*an*, cioè la possibilità o meno di impiegare il captatore, bensì il *quomodo*, ovverosia l'individuazione dei limiti al suo utilizzo. La materia, come già detto, è incandescente, onde per cui il legislatore è chiamato a muoversi con cautela per individuare un punto di equilibrio tra esigenze repressive e tutela dei diritti fondamentali.

C) *Quid iuris* nel caso in cui la polizia giudiziaria intenda apprendere il contenuto di una comunicazione che è stata correttamente presa in carico dal "dispositivo ricevente", ma non è ancora giunta a conoscenza del soggetto (persona fisica) al quale era indirizzata? La risposta al quesito dipende dall'esegesi che si intende offrire del concetto di "flusso comunicativo", giacché solo qualora si ritenga che, in detta ipotesi, la propalazione di dati digitali sia ancora *in fieri*, potrà ragionevolmente invocarsi la regolamentazione prevista all'art. 266-*bis* c.p.p. La disciplina in tema di intercettazioni (anche telematiche), infatti, può trovare applicazione solo qualora la captazione avvenga in tempo reale, cioè contestualmente all'atto comunicativo. In caso contrario, le informazioni possono essere acquisite solamente attraverso il sequestro del supporto fisico che le contiene (artt. 253 o 354 c.p.p.).

A tal proposito, occorre tentare di fare chiarezza.

L'oggetto delle intercettazioni telematiche non è costituito, come potrebbe a prima vista risultare, dai *bit* digitali che transitano in Rete, bensì, come si evince dalla lettura dell'art. 266-*bis* c.p.p., da un «flusso di comunicazioni», cioè, da un transito di materiale informativo[160]. Inoltre, nell'attuale contesto sociale governato dall'*hi-tech*, come si è detto,

---

[157] Sul concetto di "intercettazione attiva", v., dal punto di vista tecnico-informatico, G. COSTABILE – S. ATERNO, *Le intercettazioni digitali*, cit., p. 342; G. VACIAGO, Digital evidence, cit. p. 83 s.

[158] La dottrina, del resto, aveva già rilevato, anni or sono, come «in una sorta di sfida dai contorni paradossali, parallelamente all'affermarsi di nuovi mezzi per corrispondere a distanza si studiano strumenti in grado di penetrare in quelle comunicazioni»: A. CAMON, *Le intercettazioni nel processo penale*, cit., p. 8.

[159] Cfr. Parte II, Cap. I, par. 1.

[160] Secondo la condivisibile posizione di S. SIGNORATO, *Le indagini digitali*, cit., p. 237, tale locuzione andrebbe intesa in senso ampio, tale da ricomprendervi «ogni dato comunicativo, quindi *e-mail*, video, foto, messaggistica, *file* sonori ed anche comunicazioni vocali».

lo scambio di parole, idee e opinioni avviene perlopiù in maniera asincronica e, perciò, in assenza di contestualità: a differenza della «comune telefonata, che suppone interlocutori dialoganti in una medesima frazione temporale», lo scambio di messaggi via *chat* avviene «in tempi distinti, con missive e risposte collocate in tempi distinti»[161].

Ne consegue, a ben riflettere, che una comunicazione può dirsi "in corso" – e, dunque, intercettabile – fino a quando il destinatario della stessa non «ha preso conoscenza del messaggio inviatogli»[162], giacché solo in quel preciso momento il compendio informativo entra nella piena disponibilità del ricevente. In altre parole, ciò che rileva, affinché si possa parlare di intercettazione, è che il flusso di comunicazione venga acquisito prima di giungere a conoscenza del destinatario (si legga, la persona fisica), perché è quello – e solo quello – l'istante in cui esso può dirsi effettivamente esaurito, in quanto l'informazione veicolata dal *device* viene effettivamente percepita dal soggetto[163]. A conferma di quanto sostenuto soccorre, altresì, l'esegesi offerta da una parte della dottrina costituzionalista in merito all'estensione cronologica della tutela apprestata all'art. 15 Cost. Secondo un'autorevole opinione, il campo di applicazione della disposizione *de qua* si estenderebbe, quantomeno, fino al momento in cui il messaggio non è «pervenuto nella sfera psichica del destinatario»[164]. È solo in quel preciso istante – si argomenta – che il ricevente ne prende effettiva conoscenza.

D) Attenzione particolare merita, infine, l'ipotesi in cui il messaggio (scritto od orale) sia stato ricevuto e letto dal destinatario, nonché, in seguito, archiviato nel proprio *device*.

A tal proposito, va sottolineato, preliminarmente, come l'effettiva presa di conoscenza dell'informazione veicolata determini, alla luce delle suesposte argomentazioni, l'inapplicabilità della disciplina prevista in tema di intercettazioni telematiche, giacché non pare potersi intravedere alcun "flusso" dinamico di dati *in fieri*.

Al fine di garantire, in ogni caso, l'apprensione di questo materiale potenzialmente rilevante per le indagini, la giurisprudenza di legittimità ha adottato un approccio particolarmente rigoroso in base al quale i messaggi *whatsapp* – al pari di quelli scambiati attraverso altre piattaforme di comunicazione – «già ricevuti e memorizzati» nel *computer* o nel telefono cellulare hanno natura documentale ai sensi dell'art. 234 c.p.p. e, pertanto, con

---

[161] Testualmente, ancorché con riguardo alla messaggistica *e-mail*, R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 130.

[162] C. PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, p. 294. Anche secondo L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, p. 11, la «segretezza della comunicazione persiste finché il destinatario, ricevuto il messaggio, ne abbia preso conoscenza. Dopo tale momento, la comunicazione cessa di essere tale per diventare eventualmente un documento».

[163] Sembrano propendere per un'esegesi tal fatta anche R.E. KOSTORIS, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in F. Ruggieri – L. Picotti (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 180, il quale osserva come «quella corrispondenza telematica inoltrata e non ancora letta dal destinatario sembrerebbe integrare proprio quel "flusso di comunicazioni" in atto che rappresenta nell'art. 266-*bis* c.p.p. il presupposto per l'attività di intercettazione»; R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, cit., p. 134; P. CORVI, *Le modalità di acquisizione dei dati informatici trasmessi mediante posta elettronica e applicativi di* chatting: *un* rebus *non ancora del tutto risolto*, in *Proc. pen. giust.*, 2023, p. 221.

[164] A. PACE, *Problematica delle libertà costituzionali. Lezioni (Parte speciale – I)*, Padova, 1985, p. 246.

riferimento a essi, non trova applicazione né la disciplina delle intercettazioni, né quella prevista all'art. 254 c.p.p.[165].

Se la soluzione adottata dai giudici appare condivisibile con riguardo alla mancata configurabilità di un'attività intercettativa – posto che, come detto, l'autorità si limita ad acquisire *ex post* un dato informatico, senza che vi sia alcun flusso di comunicazione in corso –, altrettanto non può dirsi, invece, in relazione alla seconda parte dell'*iter* argomentativo. Ciò che non convince, giova chiarirlo, non è tanto l'impossibilità di applicare la regolamentazione prevista all'art. 254 c.p.p. in tema di sequestro, bensì l'affermazione secondo cui i messaggi rinvenuti nelle *chat* «non rientrano nel concetto di corrispondenza, la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi».

E si spiega.

La disposizione in esame, al pari dell'art. 254-*bis* c.p.p., è destinata a trovare applicazione solamente con riguardo alla corrispondenza ubicata presso terzi, ovverosia gli enti gestori che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni. La norma, al contrario, non può operare allorquando, come nel caso di specie, si tratti di imporre un vincolo permanente su una *res* (analogica o digitale) in possesso dell'indagato[166]. Inoltre, l'oggetto del sequestro di cui all'art. 254 c.p.p. è individuato nella corrispondenza *in itinere*, cioè in un momento in cui i messaggi sono ancora in transito dal mittente al destinatario. Si è detto, però, che una delle caratteristiche proprie delle nuove piattaforme digitali di comunicazione è la ricezione istantanea e in tempo reale dei messaggi inviati dal mittente e la loro ricezione, pressoché immediata, da parte del ricevente. Diviene sostanzialmente impraticabile, pertanto, un sequestro di dati *in fieri ex* art. 254 c.p.p., giacché questi permangono nell'etere solo per pochi secondi[167].

Escludere le comunicazioni *Whatsapp* dal campo di applicazione dell'art. 254 c.p.p. non significa, tuttavia, avallare l'idea – di matrice pretoria – secondo la quale ogni comunicazione esaurita, cioè, giunta a conoscenza del destinatario, non dovrebbe essere qualificata come "corrispondenza", bensì alla stregua di un semplice documento.

---

[165] L'orientamento è consolidato. Cfr., *ex plurimis*, Cass. pen., Sez. V, 14 febbraio 2023, n. 24824; Cass. pen., Sez. II, 1° luglio 2022, n. 39529; Cass. pen., Sez. V, 21 novembre 2017, n. 1822.

[166] Concordi anche F. ZACCHÈ, *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 2013, p. 109; M. TORRE, Whatsapp *e l'acquisizione processuale della messaggistica istantanea*, in *Dir. pen. proc.*, 2020, p. 1279 ss.

[167] Per una diversa impostazione, v., invece, R. DEL COCO, *L'utilizzo probatorio dei dati* whatsapp *tra lacune normative e avanguardie giurisprudenziali*, in *Proc. pen. giust.*, 2018, p. 541, la quale, proprio in ragione della contestualità che contraddistingue i tempi di inoltro e ricezione dei messaggi, propone una «"calibratura interpretativa"» dell'art. 254 c.p.p. «volta ad estendere la nozione di corrispondenza [*ivi* contenuta] a tutti quei dati digitali (messaggi sms, *whatsapp*, *e-mail*) già pervenuti al destinatario».

Secondo la convincente opinione recentemente espressa dalla Corte costituzionale[168] – e già avanzata da attenta dottrina[169] –, lo scambio di messaggi elettronici (attraverso *Whatsapp*, *Messanger*, etc.) rappresenta, di per sé, una vera e propria forma di corrispondenza tutelata dalla Carta delle Leggi. Diversamente opinando – cioè, degradare la comunicazione e mero documento quando non più *in itinere* –, si finirebbe per relegare in «ambiti angusti la tutela costituzionale prefigurata dall'art. 15 Cost.»[170], affermandone l'applicabilità solo con riguardo a quella forma di corrispondenza, cartacea, che, nell'attuale momento storico, assume indubbiamente un ruolo di secondo piano.

La conclusione, a ben considerare, si giustifica alla luce della distinzione tra i concetti di "corrispondenza attiva/dinamica" e "corrispondenza statica". Si vuol dire, cioè, che i messaggi già inviati, pervenuti al destinatario e sincronizzati sul proprio dispositivo non divengono, per ciò solo, assimilabili a un qualunque altro documento digitale[171], bensì mantengono la natura di corrispondenza, ancorché, precisamente, statica. Questo assunto si impone in ragione del fatto che la presa visione della comunicazione da parte del destinatario non incide sulla garanzia apprestata dall'art. 15 Cost. che, al contrario, permane finché il decorso del tempo non trasforma quel «messaggio in un documento "storico", avente carattere meramente retrospettivo»[172]. Per tale ragione, non può essere condivisa l'esegesi – pur avallata da autorevole dottrina[173] – in base alla quale la semplice visualizzazione del messaggio (e la successiva archiviazione nel *device*) provocherebbe l'esaurimento dell'atto di corrispondenza e, di riflesso, il venir meno della segretezza.

Alla luce di quanto osservato, sembra possibile affermare che le comunicazioni ricevute, lette e conservate nel dispositivo del destinatario rientrano a pieno titolo nel campo di operatività dell'art. 15 Cost.; esse, perciò, sono inviolabili e possono essere apprese dall'autorità inquirente solamente in presenza di una legge che legittimi l'ingerenza e di un provvedimento motivato che assicuri un equo contemperamento tra il diritto alla segretezza e l'interesse alla repressione dei reati. Da questo punto di vista, perciò, la prassi giudiziaria volta al sequestro ordinario del *device ex* art. 253 c.p.p., al fine di apprendere il contenuto della messaggistica *ivi* incorporata, deve ritenersi *contra Constitutionem*, posto che la

[168] Corte cost., 22 giugno 2023, n. 170. Sulla pronuncia, cfr., tra i molti, D. CURTOTTI, *La sentenza costituzionale n. 170 del 2023 e le comunicazioni "apparenti": quando un eccesso di garanzie non sempre è un moltiplicatore di garanzie*, in *Dir. inf. e informatica*, 2023, p. 708 ss.; L. LUPÁRIA – F. CERQUA, *La versione della consulta sulla corrispondenza elettronica. Un* bouleversement *in materia di prova digitale?*, in *ivi*, 2023, p. 718 ss.

[169] F. ZACCHÈ, *L'acquisizione della posta elettronica nel processo penale*, cit., p. 110, per il quale «la posta elettronica già letta e archiviata dal destinatario nell'apposita cartella, finché attuale, risulta coperta dall'art. 15 Cost. e, come tale, andrebbe assunta». Nello stesso senso, v. pure P. TROISI, *Le investigazioni digitali sotto copertura*, Bari, 2022, p. 188.

[170] Corte cost., 22 giugno 2023, n. 170, cit., par. 4.4.

[171] *Contra* E.M. MANCUSO, *L'acquisizione di contenuti* e-mail, in A. Scalfati (a cura di), *Le indagini atipiche*, cit., p. 517, per il quale la «corrispondenza statica» appare «del tutto assimilabile a ogni altro documento digitale».

[172] È la tesi notoriamente sostenuta da P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., p. 164.

[173] Per tutti, A. PACE, *Art. 15 Cost.*, in A. Branca (a cura di), *Commentario alla Costituzione*, Bologna-Roma, 1977, p. 85; V. ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni*, Torino, 1963, p. 212.

riconducibilità di dette informazioni nella nozione di corrispondenza – ancorché esaurita – impone il rispetto della riserva di giurisdizione[174].

7. Tutela dei minori e cybersorveglianza delle *chat* di *instant messaging*: derive orwelliane della "Piccola Europa"

Nell'ambito della complessiva "Strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori"[175] e contestualmente all'adozione dell'*European strategy for a better internet for kids (BIK+)*[176], la Commissione europea ha presentato l'11 maggio 2022 una Proposta di Regolamento recante norme per la prevenzione e il contrasto agli abusi sessuali *online* commessi nei confronti di soggetti non ancora maggiorenni[177].

In linea di continuità con il precedente Regolamento UE 2021/1232[178] e nel condivisibile intento di arginare un fenomeno in costante crescita negli ultimi anni – come dimostrano, inequivocabilmente, i numerosi *report* in materia[179] –, il provvedimento ambisce a individuare norme uniformi per contrastare l'utilizzo dei servizi della società dell'informazione per la commissione di «attività illecite a danno di minori». All'interno di tale categoria rientrano, per espressa previsione legislativa, tre differenti condotte, qualificate in termini di «abuso sessuale su minori *online*». Trattasi, in dettaglio, della diffusione di materiale precedentemente individuato e confermato come materiale pedopornografico (cd. materiale pedopornografico noto) o di materiale non precedentemente rilevato che potrebbe costituire materiale pedopornografico, ma che non è stato ancora confermato come tale (cd. materiale pedopornografico nuovo), nonché della realizzazione del cd. *cyber-grooming* (adescamento di minore).

Nel perseguire tali finalità, la proposta, al pari di quanto previsto nel *Digital Service Act*[180], muove dal presupposto che i prestatori di servizi di *hosting* svolgano un ruolo fondamentale nel rendere la Rete un luogo più sicuro e, di riflesso, per implementare attività di contrasto

---

[174] A conclusioni non dissimili sembrerebbe giungere pure F.R. DINACCI, *I modi acquisitivi della messaggistica* chat *o* e-mail*: verso letture rispettose dei principi*, in *Arch. pen.* web, 2024, p. 26. In senso contrario, però, si è recentemente espressa una pronuncia del Tribunale di Milano, la quale, pur richiamando il *dictum* espresso dalla Corte costituzionale nella sentenza n. 170/2023, ha stabilito «che la tutela apprestata dall'art. 15 Cost. alla corrispondenza, comprensiva di *mail*, *sms* e messaggi *WhatsApp*, richiede soltanto il sequestro da parte del Pubblico Ministero, secondo la procedura stabilita dagli art. 253 ss. c.p.p.» (cfr. Tribunale di Milano, Sezione VII penale, Ordinanza, 5 dicembre 2023, in *Giur. pen.* web, 11 dicembre 2023).

[175] "Strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori", COM(2020) 607 final, 24 luglio 2020.

[176] "Un decennio digitale per bambini e giovani: la nuova strategia europea per un'internet migliore per i ragazzi" (BIK+) COM(2022) 212 final, 11 maggio 2022.

[177] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori COM(2022) 209, 11 maggio 2022.

[178] Regolamento (UE) 2021/1232 del Parlamento europeo e del Consiglio del 14 luglio 2021 relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali *online* sui minori. La proposta in esame, come è dato leggere nel considerando n. 78, ricorda che il predetto Regolamento (UE) 2021/1232 costituisce una soluzione temporanea per quanto riguarda l'impiego di tecnologie ai fini della lotta contro l'abuso sessuale su minori *online*, in attesa della preparazione e adozione di un quadro giuridico a lungo termine, rappresentato, per l'appunto, dalla proposta di Regolamento di cui in oggetto. Viene auspicata, pertanto, l'abrogazione della precedente disciplina, ovverosia del Regolamento (UE) 2021/1232.

[179] *https://www.weprotect.org/economist-impact-global-survey/*.

[180] Cfr. Parte II, Cap. II.

alla pedopornografia virtuale e alla circolazione di immagini e video di abusi commessi su soggetti non ancora maggiorenni. Si è preso atto, in altre parole, di un dato che dovrebbe rappresentare una costante in ogni riflessione relativa al tema della *cyber-regulation*[181] e, a maggior ragione, della *cybercrime investigation*: i SNP sono soggetti (privati) con i quali le autorità statali debbono necessariamente interloquire per tentare di governare i fenomeni *online*, ovvero garantire i diritti dei cibernauti e, al contempo, le esigenze conoscitive delle autorità inquirenti.

Sennonché, il giudizio positivo e senza riserve manifestato con riguardo agli intenti perseguiti dalla recente proposta deve essere rimeditato allorquando si analizzi nel dettaglio il contenuto del *corpus* normativo e, in specie, la scelta degli strumenti utilizzati per garantire un efficace contrasto alla criminalità minorile. Da questo punto di vista, il Regolamento, non a caso denominato "*ChatControl*", rappresenta, così per come attualmente strutturato, una forma perversa e legalizzata di "sorveglianza preventiva di massa" che legittima gli Stati membri a realizzare, in espressa deroga a quanto stabilito dall'art. 5 della Direttiva *e-privacy*[182], un controllo sistematico delle *chat* (anche quelle protette da crittografia *end-to-end*) di tutti gli utilizzatori dei servizi di *real-time conversations* (e non solo). La proposta desta ancor più scalpore dal momento proviene da un'Istituzione, quella europea, che tra i valori fondatori annovera proprio la salvaguardia delle libertà fondamentali dei suoi cittadini.

E si spiega.

In linea generale, la proposta è volta ad attribuire specifici obblighi in capo ai fornitori di servizi che consentono lo scambio diretto, interpersonale e interattivo di informazioni, tra i quali possono essere annoverati, dunque, anche – e, verrebbe da dire, specialmente – i *Social network provider* e le relative piattaforme di *instant messanging* (*Whatsapp, Snapchat*, etc.).

Da un lato, l'art. 3 obbliga detti soggetti allo svolgimento di un'"attività di mappatura dei rischi", cioè una valutazione, per ciascun servizio offerto, dei possibili pericoli connessi a un loro uso improprio a fini di abuso sessuale su minori realizzato *online*, adottando, se del caso, tutte le misure idonee per ridurre al minimo il verificarsi di simili eventi (art. 4).

A fronte di questa (legittima e doverosa) attività proattiva, vi è, dall'altro lato, l'attribuzione di una funzione *lato sensu* inquirente che desta non poche preoccupazioni sul versante procedimentale e sulla quale occorre soffermare l'attenzione.

L'art. 7, in particolare, si propone di introdurre l'istituto del cd. ordine di rilevazione (*detection order*), a mente del quale «l'autorità coordinatrice del luogo di stabilimento» – cioè, un'autorità istituita *ad hoc* in ogni Stato membro, competente per tutte le materie

[181] Cfr. Parte I, Cap. I, par. 3.

[182] Trattasi, come noto, della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. L'art. 5, in particolare, istituisce un divieto generalizzato di ascoltare, captare, memorizzare, intercettare e sorvegliare le comunicazioni e i dati sul traffico in capo a persone diverse dagli utenti, senza il consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'art. 15, par. 1. Disposizione, quest'ultima, che consente agli Stati membri di adottare disposizioni legislative volte a limitare tale garanzia qualora la restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè, della sicurezza dello Stato), della difesa, della sicurezza pubblica e la prevenzione, la ricerca, l'accertamento e perseguimento dei reati.

connesse all'applicazione e all'esecuzione del Regolamento[183] – può ordinare all'autorità giudiziaria (o ad altra autorità amministrativa indipendente) dello Stato membro di emettere un ordine di rilevazione che impone a un prestatore di servizi di adottare le misure tecnologiche adeguate per rilevare casi di abuso sessuale su minore realizzati in un servizio specifico (ad esempio, *Whatsapp*). Queste misure consistono, in estrema sintesi, nell'installazione di un sistema di analisi e "scansione" automatizzata delle conversazioni intrattenute fra gli utenti, con il fine di individuare materiale pedopornografico.

Invero, i modelli di cd. "moderazione algoritmica dei contenuti" differiscono a seconda del tipo di *bit* che si voglia identificare. È possibile, anzitutto, operare mediante un raffronto automatico dei *file* inviati con un *database* di riferimento, cosicché qualora vi sia riscontro tra un *hash* individuato dall'algoritmo e uno già presente nella banca dati, il servitore provvederà a segnalarlo alle autorità competenti. Qualora, invece, risulti necessario rintracciare il cd. materiale pedopornografico nuovo o le condotte di *cyber-grooming*, il SNP deve ricorrere a sofisticati strumenti di *machine learning* in grado di analizzare il contenuto semantico delle *chat* e il significato delle comunicazioni audio e video, al fine di stabilire se esse abbiano o meno carattere illecito.

Alla luce del quadro normativo appena descritto, sorgono spontanee alcune considerazioni.

Si è detto, in precedenza, come l'impiego di tecnologie e *software* diretti a filtrare automaticamente possibili contenuti pedopornografici, terroristici e, più in generale, illegali presenti in Rete sia già stato implementato dalle grandi *Companies* del *web*. *Facebook*, ad esempio, utilizza modelli di intelligenza artificiale per rilevare immagini e video aventi precisamente un contenuto pedopornografico[184]. Si tratta, però, di operazioni realizzate con esclusivo riferimento a dati *open access*, rispetto ai quali, perciò, le istanze di riservatezza possono ritenersi soccombenti a fronte di un legittimo pattugliamento operato dai SNP per garantire la sicurezza digitale.

Con la proposta in oggetto, invece, si pretende di estendere simili attività pure a tutte le informazioni segrete che circolano attraverso le applicazioni di messaggistica istantanea, gli *accounts social* privati, gli spazi *Cloud*, nonché le comunicazioni scambiate, ad esempio, nei "gruppi chiusi" di *Facebook*.

Della differente capacità intrusiva che connota le attività appena richiamate sembra essere pienamente consapevole lo stesso legislatore comunitario che, nella valutazione di impatto sui diritti fondamentali contenuta nella proposta[185], sottolinea come la previsione di un obbligo di rilevazione dei contenuti illeciti nel contesto dei servizi «rivolti al pubblico» – cioè, realizzati in «spazi pubblici virtuali» – e in quelli destinati ai privati «implica diversi livelli di invasività rispetto ai diritti fondamentali degli utenti». Ciò nonostante, i *conditores* assumono che la natura «particolarmente grave» dei delitti in questione giustifichi, ai sensi dell'art. 52, par. 1, della Carta, una deroga agli artt. 5, par. 1 e 6, par. 1 della Direttiva 2002/58/CE, volti a tutelare il diritto al rispetto della vita privata e la riservatezza delle

[183] …e chiamata ad assolvere i propri compiti con obiettività, imparzialità, trasparenza e indipendenza (artt. 25 e 26).

[184] Si possono citare, ad esempio, i sistemi PDQ, TMK+ e PDQF.

[185] Proposta di Regolamento, cit., p. 13.

comunicazioni. La proposta di Regolamento – si sostiene – offre una valida e idonea base legale per una loro limitazione.

Questa prospettiva, però, non appare affatto convincente.

Il monitoraggio e la scansione dei dati riguarderebbero tutti gli utenti, senza distinzione tra *account* precedentemente segnalati, specifiche utenze o zone geografiche, né, tantomeno, queste attività sarebbero circoscritte a persone specificamente sospettate di aver commesso un reato. In assenza di un esplicito riferimento al criterio di proporzionalità, appare evidente come il controllo realizzato dai SNP risulti in tutto e per tutto equiparabile a una sorveglianza di massa; un'operazione rispetto alla quale, come noto, la Corte di giustizia ha manifestato un atteggiamento di netta chiusura, sottolineando come quest'ultima risulti incompatibile con i diritti fondamentali alla vita privata e alla protezione dei dati personali sanciti dalla Carta[186].

Né, a fugare tale pericolo, potrebbero concorrere le generiche indicazioni contenute nel terzo capoverso dell'art. 7 della proposta, a mente del quale l'autorità giudiziaria o l'autorità amministrativa indipendente può emettere un ordine di emissione nel caso in cui risulti comprovata l'esistenza di un rischio significativo che il singolo servizio messo a disposizione dal *provider* sia usato a fini di abuso sessuale su minori (*i*) e i motivi per emettere l'ordine di rilevazione siano ritenuti prevalenti sulle conseguenze negative per i diritti e gli interessi legittimi di tutte le parti interessate (*ii*). Si tratta, all'evidenza, di parametri oltremodo generici e financo tautologici che rischiano di dar vita a un'applicazione del tutto discrezionale della normativa, specialmente considerando l'assenza di limiti di carattere temporale[187].

Non è fuor d'opera sottolineare, inoltre, come gli strumenti di intelligenza artificiale in grado di rilevare la presenza di contenuti pedopornografici siano affetti da margini di errore assai rilevanti. Benché debba effettivamente riconoscersi che i modelli di *hash detection* sono connotati da un ridotto intervallo di confidenza, i falsi positivi nel caso di impiego dei *tools* di *machine learning* rappresentano, invece, una costante di queste tecnologie[188], con la conseguenza che un cittadino potrebbe essere segnalato per una presunta diffusione di materiale illecito successivamente rivelatosi pienamente legale. Se solo si considera, ad esempio, che su *Whatsapp* vengono scambiati, in tutto il mondo, mediamente 100 miliardi di messaggi al giorno, è agevole comprendere come anche una percentuale di errore dell'1-2% – tutt'altro che inverosimile – comporterebbe una quantità enorme di segnalazioni erronee. Si fa concreto, da questo punto di vista, il rischio che comunicazioni riservate e giuridicamente irrilevanti siano visualizzate dal personale che lavora presso le grandi

[186] V., per tutte, CGUE, 8 aprile 2014, *Digital Rights Ireland*, par. 39.

[187] Solo qualora il periodo di applicazione dell'ordine di rilevazione superi i 12 mesi, oppure i sei mesi nel caso degli ordini di rilevazione per adescamento di minori, l'art. 9, comma 3 stabilisce che l'autorità coordinatrice del luogo di stabilimento imponga al *provider* di riferire sull'esecuzione del medesimo quanto meno una volta, a metà del periodo di applicazione.

[188] Lo rilevano, esplicitamente, R. GORWA – R. BINNS – C. KATZENBACH, *Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance*, in *Big Data & Society*, 2020, 7, p. 1 ss.

Companies del *web*, inoltrate all'autorità giudiziaria e, nel peggiore dei casi, "hackerate" da esperti informatici.

A nulla varrebbe, in proposito, il richiamo operato dalla proposta al principio di neutralità tecnologica: le strumentazioni di rilevazione – si afferma – dovrebbero essere in grado di garantire, indipendentemente dai singoli *software* impiegati, gli *standards* previsti nella bozza di regolamento[189]. Nonostante siano in via di sviluppo sistemi in grado di scansionare – esclusivamente mediante tecnica di *hash* – il testo delle comunicazioni private, senza, però, consentire a terzi di dedurne il contenuto[190], non sembra che la scienza informatica possa ad oggi garantire sul mercato strumenti capaci di adeguarsi agli stringenti parametri indicati dal Regolamento[191]. Insomma, allo stato attuale, il rischio che miliardi di conversazioni private possano essere apprese ed archiviate da terzi non autorizzati è tutt'altro che inverosimile.

Si è detto, peraltro, che la proposta riguarda specialmente i servizi di comunicazione criptata *end-to-end*, quali sono la maggior parte delle piattaforme di messaggistica istantanea messe a disposizione dai SNP. Per garantire comunque la possibilità "scannerizzare" le conversazioni private, i *provider* saranno obbligati a creare delle *backdoor*, cioè delle "vie telematiche nascoste" che consentano di accedere alle informazioni contenute nelle *chat*. Una volta infranto il muro sella segretezza – occorre esserne consapevoli – non è possibile garantire che queste "strade segrete" non vengano percorse da malintenzionati (o dalle agenzie di *intelligence* criminale) per acquisire in massa i dati *ivi* contenuti[192].

Nessuno dubita, è opportuno precisarlo, che i sistemi E2EE *service*, sebbene essenziali nella moderna società tecnologica per garantire la libertà e la segretezza delle comunicazioni, rischino di creare uno spazio franco, un paradiso cibernetico nel quale i delinquenti possono svolgere le proprie attività delittuose al riparo dagli occhi indiscreti dell'autorità. Ciò che colpisce, però, è il disinteresse mostrato dalle Istituzioni europee per la tutela dei sistemi di

[189] Ai sensi dell'art. 10, commi 3, 4, le tecnologie devono essere «a) efficaci nel rilevare la diffusione di materiale pedopornografico noto o nuovo o l'adescamento di minori, a seconda dei casi; b) non in grado di estrarre dalle comunicazioni in questione informazioni diverse da quelle strettamente necessarie per rilevare, a mezzo degli indicatori di cui al paragrafo 1, pattern rivelatori di diffusione di materiale pedopornografico noto o nuovo o di adescamento di minori, a seconda dei casi; c) in linea con lo stato dell'arte del settore e le meno intrusive in termini di ingerenza nei diritti degli utenti al rispetto della vita privata e familiare, compresa la riservatezza delle comunicazioni, e alla protezione dei dati personali; d) sufficientemente affidabili da limitare al massimo il margine di errore di rilevazione. Il prestatore: a) deve prende tutti i provvedimenti del caso per garantire che le tecnologie e gli indicatori, al pari del trattamento dei dati personali e altri dati a questi connessi, siano usati al solo fine di rilevare la diffusione di materiale pedopornografico noto o nuovo o l'adescamento di minori, a seconda dei casi, nella misura strettamente necessaria per eseguire l'ordine di cui è destinatario; b) istituisce procedure interne effettive per prevenire e se del caso rilevare e correggere l'uso improprio delle tecnologie, degli indicatori e dei dati personali e altri dati di cui alla lettera a), compreso l'accesso non autorizzato agli stessi e loro trasferimenti non autorizzati; c) deve prevede la vigilanza umana periodica necessaria per garantire che le tecnologie funzionino in misura sufficientemente affidabile e se necessario l'intervento umano, in particolare quando sono rilevati errori potenziali e un potenziale adescamento di minori».

[190] Si veda, ad es., il modello elaborato da alcuni ricercatori dell'Università di Princeton presentato alla 30th USENIX Security Symposium, USENIX Security, 2021 (*https://collaborate.princeton.edu/en/publications/identifying-harmful-media-in-end-to-end-encrypted-communication-e*).

[191] R. GORWA – R. BINNS – C. KATZENBACH, *Algorithmic content moderation*, cit., p. 1 ss.

[192] Sono evidenti, in proposito, gli effetti deterrenti e pregiudizievoli prodotti sulla libertà di comunicazione e di manifestazione del pensiero, cd. *chilling effect*. Cfr. CGUE, 6 ottobre 2020, *La Quadrature du Net*.

cifratura; un'indifferenza che merita di essere censurata, specialmente a fronte dell'ultimo *report* dell'Alto Commissario per i Diritti Umani presso le Nazioni Unite, titolato «*The right to privacy in the digital age*»[193]. Nel documento si afferma che l'*encryption* rappresenta un elemento chiave, nell'era moderna, per garantire la libertà delle comunicazioni e si sottolinea che gli Stati debbano tendenzialmente astenersi dall'interferire con simili tecnologie[194]. Di più: nell'atto si critica apertamente la scelta di quegli ordinamenti che hanno imposto obblighi generali di vigilanza in capo ai *provider* consistenti nella realizzazione di *backdoor*, dal momento che nella totalità dei casi – si rileva – le misure risultano sproporzionate e lesive della privatezza dell'intera popolazione, senza che vi siano distinzioni di sorta, proprio come accade, lo si è visto, nella proposta in esame. Peraltro, è lo stesso Comitato per i diritti dell'infanzia ad aver auspicato, in un recente *report* sulla salvaguardia dei diritti dei minori in ambiente digitale[195], che qualunque misura volta a individuare e mappare contenuti illeciti ipoteticamente presenti in sistemi di comunicazione chiusa e crittografati debba sottostare ai principi di legalità, necessità e proporzionalità dell'intrusione; in caso contrario, il peso imposto alle libertà dei singoli, pur legittimato dal perseguimento di uno scopo legittimo, sarebbe irragionevole e, dunque, democraticamente insostenibile.

Nella speranza, perciò, che i moniti dell'Alto Commissario abbiano un qualche eco a livello europeo, e sulla scia delle preoccupazioni manifestate anche dal Presidente del Garante italiano per la protezione dei dati personali[196] (ed emergenti, altresì, da recenti sondaggi a livello comunitario[197]), non resta che auspicare un intervento del Parlamento volto a contrastare (o, quantomeno, rimodulare) l'*iter* di approvazione di questa deludente proposta legislativa.

È doveroso precisare, tuttavia, che le critiche qui mosse nei confronti dell'attuale *draft* normativo non devono indurre a censurare qualsivoglia impiego di *tools* "auto-intelligenti", specie nel contesto procedimentale *strico sensu* inteso. La necessità di accertare la commissione di delitti contro soggetti minori d'età potrebbe essere perseguita, nel rispetto delle garanzie fondamentali della persona e del canone di proporzionalità, mediante l'utilizzo di sistemi di IA che, alla sussistenza di specifici presupposti legali, possano essere inoculati (un po' come avviene per il *trojan*) con l'esclusiva finalità di individuare materiale pedopornografico eventualmente presente nelle *chat* private in uso a determinate persone identificate *ex ante*. In questo modo, l'attività intrusiva sarebbe soggettivamente limitata nei

[193] REPORT OF THE OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS, *The right to privacy in the digital age*, 4 agosto 2022, spec., parr. 20-28.

[194] Nella "Sezione *Privacy*" di *Whatsapp*, peraltro, il "colosso del *web*" da conto del carattere essenziale, nella moderna società tecnologica, ricoperto dai sistemi di cifratura, anche e specialmente per far fronte ad attacchi cibernetici che rischiano di mettere a repentaglio i diritti degli utenti: «la sicurezza è essenziale per il servizio che fornisce *WhatsApp*. Abbiamo assistito a diversi casi in cui degli *hacker* hanno ottenuto illegalmente grandi quantità di dati privati e hanno abusato della tecnologia per danneggiare le persone usando le informazioni personali rubate. Da quando è stata completata l'implementazione della crittografia *end-to-end* nel 2016, la sicurezza digitale è diventata ancora più importante» (*https://faq.whatsapp.com/820124435853543/?locale=it_IT*).

[195] COMMITTEE ON THE RIGHTS OF THE CHILD, *General comment No. 25 (2021)*, 2 marzo 2021.

[196] *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9688789*.

[197] *https://www.patrick-breyer.de/en/poll-72-of-citizens-oppose-eu-plans-to-search-all-private-messages-for-allegedly-illegal-material-and-report-to-the-police/*.

confronti di coloro che risultano destinatari di indizi a carico e oggettivamente circoscritta al solo rilevamento di materiale illecito: un giusto equilibrio tra finalità repressive e tutela della libertà e della segretezza delle comunicazioni.

8. Il ruolo dei *Social network provider* nell'apprensione delle informazioni segrete: verso un'esternalizzazione consapevole (e necessaria) della funzione perquirente

Com'è stato osservato dai più attenti commentatori, il moderno rito criminale è caratterizzato da una generale tendenza alla privatizzazione nella gestione del conflitto scaturente dal reato (la mente corre, *in primis*, alle procedure penali negoziate/consensuali)[198] e all'esternalizzazione nello svolgimento di determinate attività processuali[199].

Naturalmente, la fase investigativa non poteva rimanere estranea a un cambiamento tanto radicale[200].

Come si è cercato di mettere in luce, a più riprese, nel corso della trattazione, vi è un aspetto che caratterizza ormai qualsivoglia indagine digitale diretta all'apprensione di informazioni contenute nei *social network*. Il riferimento va al ruolo centrale assunto dai *provider*, soggetti privati che nel libero esercizio di un'attività economica (*rectius*, la commercializzazione di servizi *hi-tech*) sono chiamati, *de facto*, a collaborare con l'autorità pubblica per rendere efficace ed efficiente l'attività investigativa. Dal momento che le informazioni a carattere riservato di utilità investigativa si trovano spesso nella disponibilità dei gestori delle piattaforme, i cui *server* sono allocati in territorio straniero (*rectius*, diverso da quello nel quale le investigazioni vengono condotte), appare inevitabile un loro coinvolgimento sin dalle prime battute delle indagini.

In realtà, sembra che le grandi *web company* vadano assumendo, a seconda dei casi, un duplice e alternativo ruolo. Come dimostrato dal noto caso *Apple c. FBI*, essi si presentano talvolta nella veste di veri e propri garanti delle libertà fondamentali degli individui, inibendo così l'esercizio del potere investigativo[201]. Talaltra, invece, i *provider* finiscono per rappresentare la *longa manus* dell'organo d'accusa. Del resto, la dottrina più attenta alla tematica *de qua* non ha mancato di mettere in luce, a quest'ultimo proposito, i vantaggi di un approccio investigativo "*provider oriented*": «mentre la polizia ha bisogno di un mandato

---

[198] Sul punto, cfr., per tutti, l'opera monografica di J. DELLA TORRE, *La giustizia penale negoziata in Europa. Miti, realtà e prospettive*, Milano, 2019.

[199] F. GASCÓN INCHAUSTI, *Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial*, in AA.VV., *La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro*, Barcellona, 2019, p. 192.

[200] Con specifico riguardo al settore in esame, v. C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, 2019, p. 1174; e, *amplius*, S. SIGNORATO, *Le indagini digitali*, cit., p. 181-204. Si pensi, altresì, al terreno delle *internal investigations* realizzate nel contesto aziendale in relazione agli illeciti amministrativi dipendenti da reato (d.lgs. 8 giugno 2001, n. 231).

[201] Il riferimento è al procedimento penale relativo all'attentato terroristico avvenuto il 2 dicembre 2015 a San Bernardino, in California. Nel corso delle indagini preliminari, gli inquirenti avevano sottoposto a sequestro un *iPhone* appartenente a uno degli attentatori. Non riuscendo ad accedere al contenuto del *device* – protetto da *password* – l'FBI aveva richiesto alla casa madre di creare un *software ad hoc* per superare il sistema di sicurezza crittografato. A fronte del diniego opposto da *Apple Inc.*, motivato dalla necessità di tutelare la *privacy* dei propri utenti, è sorta una vera e propria *querelle* giudiziaria.

per accedere ai dati privati di qualcuno, *Facebook* può esaminare i dati dei suoi utenti quando vuole»; cosicché, per il pubblico ministero «potrebbe essere un gran vantaggio se a fare il lavoro sporco fosse *Facebook*, dato che il suo sistema investigativo non deve passare attraverso i meccanismi giudiziari»[202].

A fronte di tale quadro, la dottrina processualista guarda pressoché con sospetto il ruolo che detti attori privati vanno via via assumendo, mettendo in guardia dal rischio che essi possano «divenire i veri depositari del potere di attuazione dell'orizzonte investigativo»[203]. Si tratta di timori tutt'altro che infondati, e il caso relativo alla cd. strage di San Bernardino ne è la prova.

Eppure, occorre forse provare a adottare un approccio realistico-pragmatico alla materia, nella convinzione che l'apporto dei *provider* risulta, nell'attuale contesto investigativo, tanto indispensabile, quanto auspicabile. Indispensabile, perché in presenza di una fase investigativa sempre più dipendente dai *bit* digitali presenti nei *social network* (*subscriber data*, *access data*, *transactional data* e *content data*), i gestori sono destinati a ricoprire un ruolo sempre più decisivo per il buon esito delle indagini[204]. Auspicabile, perché la titolarità, *de facto*, in capo ai *provider* di uno *ius investigandi* comporta, in assenza di una regolamentazione circa la modalità di esercizio di detto potere, un *deficit* di controllo democratico sull'amministrazione della giustizia[205]. Soggetti privati, difatti, sono in grado di determinare il buon esito o meno delle indagini, del processo e, di riflesso, dello *ius punendi*.

In questo contesto, gli strumenti tradizionali pensati per consentire un'apprensione transfrontaliera di prove allocate oltre i limi territoriali di uno Stato (si legga, la rogatoria) si rivelano oggi (e, invero, già da tempo) del tutto inadeguati. Neppure i meccanismi di cooperazione più evoluti a livello eurounitario possono definirsi appropriati: la lentezza che caratterizza la procedura di emissione dell'ordine europeo di indagine penale costituisce ormai un "fatto notorio"[206].

Se un tanto è vero, debbono essere accolte con favore le numerose iniziative promosse a livello europeo dirette a coinvolgere direttamente i *provider*, attraverso una puntuale

---

[202] Così, richiamando le parole di Eugeny Morotzov, L. LUPÁRIA, *Il sistema penale ai tempi dell'*Internet. *La figura del provider tra diritto e processo*, in Id (a cura di), Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, p. 9.

[203] S. SIGNORATO, *Le indagini digitali*, cit., p. 182. Esprime, in termini generali, il timore per il possibile coinvolgimento dei *provider* nella fase di ricerca della prova, M. DANIELE, *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. Direito Processual Penal*, 2019, p. 1277 ss.

[204] Come messo esplicitamente in luce da S. SIGNORATO, *Tipologie e caratteristiche delle* cyber investigations *in un mondo globalizzato*, in *Dir. pen. cont. – Riv. Trim.*, 2016, 3, p. 198, «*the cooperation with private parties is an absolute prerequisite for an effective investigation activity aimed at combating cybercrime and for gathering digital evidence for any crime. In general, such a cooperation cannot be avoided*».

[205] T. ARMENTA DEU, *Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambio*, Madrid, 2021, p. 301 s.

[206] Lo mettono in luce, tra i molti, M. DANIELE, *L'acquisizione delle prove digitali dai* service provider, cit., p. 1279-1281; M. GIALUZ – J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. cont.*, 2018, 5, p. 281.

regolamentazione, nell'assistenza allo svolgimento delle indagini digitali[207]. È in detto contesto che vengono a collocarsi il recente Regolamento europeo *e-evidence*[208] e il II protocollo addizionale alla Convenzione di Budapest sul *Cybercrime*[209]. Pur a fronte del diverso ambito di applicazione e dei (numerosi) difetti a livello contenutistico, entrambe le fonti sovranazionali muovono da una precisa e condivisibile convinzione di fondo: l'implementazione di un dialogo costruttivo tra i *social network provider* e le autorità investigative rappresenta la via più rapida ed efficace per contrastare la nuova criminalità del XXI secolo, rispetto alla quale l'acquisizione delle informazioni estrapolate dalle piattaforme di *sharing* va acquisendo un peso sempre maggiore. Si tratta, come puntualmente osservato, di un vero e proprio «cambio di paradigma»[210] nella gestione della prova informatica transfrontaliera: si è passati, cioè, da una modello basato su una collaborazione Stato richiedente-Stato richiesto a una nuova idea di collaborazione Stato-*provider*. L'idea di disciplinare, in via legislativa, quella che, nella prassi, si mostra, il più delle volte, come una sorta di "delega pubblica della funzione di repressione penale" è sintomo di una presa di coscienza del *lawmaker* comunitario che deve essere apprezzata.

Con ciò, è opportuno precisarlo, non si intende sostenere – come pur proposto da accreditati studiosi – la necessità di ripensare e ridefinire il concetto di «autorità di persecuzione penale», al fine di includervi, in una certa maniera, pure i SNP, attribuendo loro una funzione intrinsecamente pubblica[211]. L'esercizio dello *ius investigandi* era, è, e deve rimanere nell'esclusiva titolarità del rappresentante d'accusa, unico soggetto al quale la Carta Fondamentale attribuisce il potere di esercizio dell'azione penale.

[207] Si mostrano favorevoli a questa nuova concezione del *modus investigandi*, M. GIALUZ – J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio*, cit., p.282, per i quali una qualche forma di collaborazione diretta tra le grandi *web company* e gli ordinamenti nazionali «consentirà finalmente ai *service provider* di cooperare in materia di prove elettroniche in un quadro giuridico chiaro e non frammentario».

[208] Regolamento (UE) 2023/1543 del Parlamento Europeo e del Consiglio del 12 luglio 2023 relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali.

[209] Si vedano i commenti pubblicati sul numero Speciale-*Cybercrime* in *Dir.pen. proc.*, 2022, 8.

[210] M. DANIELE, *L'acquisizione delle prove digitali dai* service provider, cit., p. 1283.

[211] È questa l'idea che sembra essere prospettata da F. GASCÓN INCHAUSTI, *Desafíos para el proceso penal en la era digital*, cit., p. 192 (trad. nostra).

PARTE III

L'IRRUZIONE DEI *SOCIAL NETWORK* NEL PROCESSO PENALE

CAPITOLO I

L'APPROCCIO STRANIERO ALLA *SOCIAL NETWORK EVIDENCE*: L'ESPERIENZA STATUNITENSE

SOMMARIO: 1. La scelta del *tertium comparationis*. – 2. *Federal Rules of Evidence*: criteri e *standard* di ammissione della prova. – 3. Alla ricerca di una disciplina organica della prova digitale: "regole analogiche" per un "mondo virtuale"? – 4. "*All evidence is equal, but some is more equal than others*": l'ingresso della *social network evidence* nel processo penale statunitense. – 4.1 Il cd. *Meryland Approach*. – 4.2 Il cd. *Texas Approach*. – 5. Manipolazione digitale e *social network platforms*: l'incursione del *deepfake* nelle aule di giustizia. – 6. Osservazioni di sintesi.

1. La scelta del *tertium comparationis*

Al fine di svolgere un approfondimento, pur breve e circoscritto, di tipo comparato, occorre, come insegna illustre dottrina, individuare un *tertium comparationis*, cioè un «problema o bisogno sociale reale condiviso dai due o più Paesi o società a cui l'analisi comparativa vuole estendersi»[1].

Nella scia dello studio che si va conducendo, questo elemento può essere individuato nella necessità di confrontarsi con la comparsa di un nuovo "materiale probatorio digitale" – ovverosia quello ricavato dai *social network* – nel processo penale e, più in particolare, nella fase dibattimentale. Se, come si è cercato di illustrare in precedenza, le autorità inquirenti, in qualunque parte del globo, ricorrono sempre più frequentemente ad attività intrusive in grado di apprendere dati presenti nelle piattaforme, ne consegue, di riflesso, un'estrema diffusività di quella che può definirsi *social network evidence*. Con tale espressione, lo si è detto, ci si riferisce all'insieme di tutte le *social media-related information*[2] – tra cui messaggi privati, *post* (pubblici o ristretti), fotografie, *tags*, commenti e altre tipologie di contenuti[3] – delle quali le parti chiedono l'ammissione in sede istruttoria.

Il secondo step dell'analisi comparata – come ricorda, nuovamente, l'Esimio processualista – consiste nell'individuare le soluzioni legislative e/o interpretative offerte dai singoli ordinamenti per tentare di risolvere il problema da essi condiviso[4].

In tal senso, lo studio dell'ordinamento e della giurisprudenza statunitense si rivela estremamente proficuo, giacché i tribunali d'oltreoceano sono stati i primi, nel panorama mondiale, a occuparsi in maniera approfondita del tema *de quo*. L'interesse per la materia va probabilmente ascritto a molteplici fattori, tra i quali può essere senz'altro annoverata la rapida diffusione, in detto contesto, di questi nuovi "mezzi di comunicazione sociale"; una diffusione che, com'era prevedibile, ha avuto importanti riflessi anche sul versante

[1] M. CAPPELLETTI, *Dimensioni della giustizia nelle società contemporanee*, Bologna, 1994, p. 17.
[2] T.A. HOFFMEISTER, *Social Media in the Courtroom. A New Era for Criminal Justice?*, Santa Barbara, 2014, p. 151.
[3] J. MEHLMAN, *Facebook and MySpace in the Courtroom: Authentication of Social Networking Websites*, in *Criminal Law Brief*, 2012, p. 11.
[4] M. CAPPELLETTI, *Dimensioni della giustizia nelle società contemporanee*, cit., p. 17.

processuale. È per tale ragione, pertanto, che uno sguardo alla cultura giuridica sviluppatasi oltreoceano può essere utile al fine di saggiare e valutare come un Paese da sempre all'avanguardia negli studi in tema di prova informatica[5] abbia affrontato (e, invero, stia tutt'ora affrontando) l'irruzione della "materia *social*" nel rito penale. La bontà di questa scelta parrebbe confermata, peraltro, da una semplice ricerca dottrinale eseguita nelle principali banche dati statunitensi: la letteratura sul punto è, allo stato attuale, già particolarmente corposa[6]. Come si avrà modo di osservare più approfonditamente, a fronte di un contrasto giurisprudenziale – e, verrebbe da dire, anche "intra-statale"[7] –, sorto tra l'approccio adottato da alcune corti del Maryland e quello fatto proprio dai tribunali del Texas, si è sviluppato un fecondo e vivace dibattito relativo alla necessità o meno di un *upgrade* normativo delle attuali regole che disciplinano, in termini generali, la fase di ammissione della prova nel processo penale statunitense.

2. *Federal Rules of Evidence*: criteri e *standard* di ammissione della prova

In ragione di quanto poc'anzi osservato, il punto d'avvio per ogni riflessione in tema di *social network evidence* nel contesto americano non può che essere rappresentato dall'analisi delle *Federal Rules of Evidence* (FRE) e, più in dettaglio, dalle disposizioni che regolano il regime di ammissione della prova in giudizio (*admisibility of evidence*). Difatti, il momento nel quale la Corte è chiamata a stabilire se quel determinato apporto conoscitivo ricavato dalle piattaforme digitali può o meno avere accesso al *trial* rappresenta, con riguardo alla prova *social*, lo *step* maggiormente critico dell'intero procedimento probatorio *lato sensu* inteso (ricerca, ammissione, acquisizione e valutazione).

Come noto, dalla lettura del combinato disposto delle *Rules* 401 e 402 FRE si ricava che le prove ammissibili nel *trial* sono solamente quelle rilevanti (*relevant evidence*), espressione con la quale il legislatore federale allude a quel compendio conoscitivo pertinente con i fatti oggetto di causa, ovverosia dotato dell'attitudine «a dimostrare l'esistenza o l'inesistenza di qualsiasi fatto ricompreso tra gli elementi costitutivi del reato oggetto del giudizio»[8]. Trattasi, in altre parole, di una valutazione che non attiene ai caratteri intrinseci della singola prova, bensì all'esistenza di un rapporto diretto o indiretto tra questa e il *thema probandum*.

[5] Ci si riferisce, in particolare, ai pioneristici saggi di Kerr.

[6] Oltre ai contributi richiamati *infra*, cfr., per una panoramica generale, J.P. MURPHY – A. FONTECILLA, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, in *Richmond Journal of Law & Technology*, 2013, p. 11-18; T.A. HOFFMEISTER, *Social Media in the Courtroom*, cit., p. 151-164.

[7] V. FANCHIOTTI, *La giustizia penale statunitense.* Procedure v. Antiprocedure, Torino, 2022, p. 33 ss.

[8] D.P. GENTILE, *Il diritto delle prove penali*, in E. Amodio – M.C. Bassiouni (a cura di), *Il processo penale negli Stati Uniti d'America*, Milano, 1988, p. 223. Di un «giudizio sulla astratta idoneità di un particolare elemento di prova ad accrescere le conoscenze della giuria intorno ai fatti per cui si procede» parla M. PAPA, *Brevi spunti sulle* Rules of Evidence, in E. Amodio – M.C. Bassiouni (a cura di), *Il processo penale negli Stati Uniti d'America*, cit., p. 362.

Il giudizio di rilevanza, così per come concepito nelle FRE, non appare particolarmente stringente. Difatti, le Corti statunitensi, in mancanza di parametri legali predeterminati[9], sono solite ricorrere al *test* della cd. *pragmatic relevance*, in base al quale debbono ritenersi irrilevanti tutti quegli elementi di prova che possono arrecare un "pericolo di ingiusto pregiudizio" per la giuria ovvero un ritardo ingiustificato nello svolgimento del processo[10]. Sotto tale profilo, l'avvento della prova *social* non sembra porre specifici problemi: è attribuito alla Corte il potere di valutare, caso per caso, se quella prova «*has any tendency to make a fact more or less probable than it would be without the evidence*»[11].

Una volta determinata la rilevanza, il secondo *step* del giudizio di ammissibilità è costituito dalla fase di autenticazione.

La norma cardine in materia è rappresentata dalla *Rule* 901(a), a mente della quale chi intende introdurre una prova in giudizio deve produrre «*evidence sufficient to support a finding that the item is what the proponent claims it is*». La *ratio* della disposizione è tradizionalmente rintracciata nella necessità di garantire l'affidabilità dell'accertamento, cioè la sua validità gnoseologica, con il precipuo scopo di evitare frodi processuali e proteggere l'imputato dal rischio di errori giudiziari[12].

Il *test* sotteso al giudizio di autenticazione è comunemente denominato *reasonable juror standard*, locuzione con la quale dottrina e giurisprudenza alludono al fatto che il proponente debba introdurre nel processo fatti o elementi che una "giuria ragionevole" riterrebbe sufficienti per supportare l'autenticità della prova della quale si chiede l'amissione[13]. La *Rule* 901(a), del resto, non specifica il *quantum* probatorio richiesto per l'autenticazione della *evidence*.

Si tratta, ad ogni modo, di un criterio variamente descritto come «*relatively low*», «*minimal*» e, ancora, «*not hight*»[14]. In effetti, il proponente non è chiamato a escludere qualunque ricostruzione alternativa circa la genuinità del dato che intende apportare, né, per converso, a dimostrarne l'autenticità oltre ogni ragionevole dubbio[15]. Egli, al contrario, deve "unicamente" convincere, *prima facie*, un "giurato-agente modello" che quella determinata prova è idonea a rappresentare ciò che la parte intende con essa sostenere.

L'indeterminatezza e la genericità di questo criterio (*reasonable juror standard*) sono in parte compensati dalla circostanza che la stessa *Rule* 901(b) individua, in via meramente

---

[9] W.G. CONLY, *Determining Relevancy: Article IV of the Federal Rules of Evidence*, in *Louisiana Law Review*, 1975, p. 71: «*the law furnishes no test of relevancy. For this, it tacitly refers to logic and general experience*».

[10] *Stati Uniti c. Clark*, 577 F.3d 273, 288 (5th Cir. 2009); *Stati Uniti c. Rocha*, 916 F.2d 219, 239 (5th Cir. 1990).

[11] *Rule* 401(a) – *Test for Relevant Evidence*.

[12] T.A. HOFFMEISTER, *Social Media in the Courtroom*, cit., p. 155.

[13] Lo *standard* del "giudice ragionevole" è illustrato nella nota sentenza *Lorraine c. Markel American Insurance Co.*, 241 F.R.D. 534, 539 (D. Md. 2007), nella quale i giudici hanno esaminato, *funditus*, la relazione tra la *Rule* 901 e la *Rule* 104(b), relativa, quest'ultima, alla disciplina generale della *relevance of evidence*.

[14] Cfr., nell'ordine, P.W. GRIMM – M.V. ZICCARDI – A.W. MAJOR, *Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information*, in *Akron Law Review*, 2009, p. 366; *Stati Uniti c. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007); *Stati Uniti c. Safavian*, 435 F. Supp. 2d 36, 38 (D.D.C. 2006).

[15] Cfr., rispettivamente, *Stati Uniti c. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007); *Stati Uniti c. Piuta*, 176 E.3d 43, 49 (2d Cir. 1999).

esemplificativa, differenti modalità di autenticazione della prova. Trattasi, più nello specifico, di un elenco "aperto" e non esaustivo[16] composto da dieci paragrafi che ricomprende, ad esempio, il riconoscimento dell'autenticità di un *quid* (un documento o un qualunque altro «*item*») attraverso la dichiarazione di un «*witness with knowledge*»[17] o la presenza, nel caso concreto, di elementi indizianti (*circumstantial evidence*[18]) o, ancora, la prova dell'avvenuta conversazione telefonica con un determinato soggetto mediante la dichiarazione proveniente da uno dei partecipanti[19].

3. Alla ricerca di una disciplina organica della prova digitale: "regole analogiche" per un "mondo virtuale"?

Alla luce di quanto osservato, non stupisce affatto l'affermazione, ricorrente nella più attenta dottrina nordamericana, secondo cui il tema dell'autenticazione rappresenta spesso «*the central battleground for determining admissibility of electronic evidence*»[20]. L'avvento della prova digitale, infatti, ha costretto interpreti e giurisprudenza a confrontarsi con un nuovo paradigma probatorio, interrogandosi sull'effettiva capacità delle FRE, introdotte nel lontano 1975, di far fronte a un fenomeno che può essere ricondotto a pieno titolo nel concetto di *Digital Disruption*[21].

Il quesito con il quale occorre confrontarsi è, invero, sempre il medesimo e tende a riproporsi, immutato, nel corso del tempo: l'evoluzione della *technè* impone un *upgrade* delle tradizionali regole processuali e, in particolare, di quelle dettate in materia probatoria o, invece, queste debbono ritenersi adeguate a fronte del "nuovo che avanza"?

Muovendo dal noto "brocardo" «*old wine in new bottles*»[22], una parte degli studiosi sostiene che «*the prevalence of electronic evidence has required no substantial changes to the Federal Rules of Evidence*»[23]. Questo indirizzo interpretativo è stato accolto nella fondamentale sentenza *Lorraine c. Markel American Insurance Co.*[24]. *Leading case* in materia, la pronuncia, oltre a sposare a pieno un approccio "conservatore", si rivela particolarmente interessante dal punto di vista processuale, giacché fornisce un vero e proprio *vademecum* al quale i giudici e gli interpreti dovrebbero attenersi nel valutare l'autenticità (e, di riflesso, l'ammissibilità) di una prova informatica.

---

[16] *Rule* 901(b) FRE: «*not a complete list*».

[17] *Rule* 901(b)(1) FRE. In base a questa regola, ad esempio, la dichiarazione di un testimone che afferma di aver visto l'imputato scrivere di proprio pugno un determinato documento sarebbe sufficiente per provarne l'autenticità, ovverosia la riconducibilità dello scritto alla "mano" dell'indagato.

[18] *Rule* 901(b)(4).

[19] *Rule* 901(b)(5). A tal proposito, ad esempio, la mera affermazione della propria identità da parte di uno dei colloquianti a distanza non è tendenzialmente ritenuta sufficiente per provare la partecipazione di quel soggetto alla conversazione.

[20] K.L. SUGISAKA, *Admissibility of E-Evidence in Minnesota: New Problems or Evidence as Usual?*, in *William Mitchell Law Review*, 2009, p. 1459.

[21] Cfr. *Introduzione*.

[22] P.N. GRABOSKY, *Virtual Criminality: Old Wine in New Bottles?*, in *Social & Legal Studies*, 2001, p. 243 ss.

[23] Così, J.D. FRIEDEN – L.M. MURRAY, *The Admissibility of Electronic Evidence under the Federal Rules of Evidence*, in *Richmond Journal of Law and Technology*, 2011, 17, p. 2. Per questa opinione, v., tra i primi, O.S. KERR, *Digital Evidence and the New Criminal Procedure*, in *Columbia Law Review*, 2005, p. 279 ss.

[24] *Lorraine c. Markel American Insurance Co*., cit.

L'argomentazione da cui muove questo indirizzo esegetico è chiara: anche se le FRE – si legga, la *Rule* 901(b) – sono state pensate e redatte avendo quale riferimento mezzi di prova analogici, molte di esse possono trovare applicazione anche con riguardo alle prove digitali. Non vi sarebbe alcuna necessità, in altre parole, di discostarsi dal modello tradizionale e dallo *standard* di ammissibilità attualmente fissato dalla legge. Va comunque notato, però, che chi abbraccia questa prospettiva mostra di essere pienamente consapevoli del fatto che le *new evidence* pongono talvolta problemi ulteriori rispetto alle prove tradizionali, in ragione della natura volatile e, per così dire, "impalpabile" dei *bit* digitali che le rende agevolmente manipolabili da chiunque e in qualunque luogo. Ciò nondimeno, viene sostenuto che le attuali FRE siano sufficienti per realizzare un adeguato e scrupoloso giudizio sull'autenticità della *electronic evidence*.

A conferma di ciò, la dottrina che avalla tale impostazione suole richiamare le ipotesi contenute ai n. 1 e 4 della *Rule* 901(b)[25]. Gli strumenti di autenticazione *ivi* previsti – si sostiene – ben potrebbero essere applicati anche con riguardo alle nuove "tipologie probatorie 2.0". Sarebbe possibile, ad esempio, che un documento elettronico venga autenticato mediante una semplice dichiarazione testimoniale (n.1) proveniente dal suo stesso autore o da un terzo. Come, parimenti, nessun ostacolo vi sarebbe alla possibilità di comprovare la genuinità di un elemento di prova e la riferibilità a un determinato soggetto attraverso un esame delle caratteristiche distintive (*circumstantial evidence*) del messaggio inviato tramite *e-mail*, come il linguaggio utilizzato o l'impiego di segni particolari (n. 4)[26].

Le riflessioni in merito alla necessità o meno di un *upgrade* normativo per far fronte all'estrema volatilità e manipolabilità del dato informatico in sede di ammissione (e valutazione) della prova digitale, in realtà, hanno interessato anche altri ordinamenti, pure di *civil law*.

Onde rendersi conto di ciò, è sufficiente volgere lo sguardo, a mero titolo esemplificativo, al dibattito – tutt'ora in corso – che si è sviluppato nella letteratura iberica. A fronte di un autorevole orientamento dottrinale che, facendo leva sulla massima *new facts will demand new law*, auspica l'introduzione di regole probatorie esclusivamente dettate per governare il fenomeno digitale[27], vi è chi, per contro, tende a ridimensionare il problema. Più in particolare, i fautori della tesi "conservatrice" sembrano muovere dal presupposto secondo cui il rischio di un'alterazione della genuinità della prova – che, nella prospettiva accolta dalla tesi avversa, giustificherebbe l'adozione di regole *ad hoc* – non riguarderebbe solamente le *new evidence*, bensì pure le prove analogiche, come nel caso della contraffazione di una firma apposta su un documento cartaceo o di una falsa testimonianza. Anzi, ribaltando un "luogo comune" diffuso tra i sostenitori della "democratizzazione della

[25] P.W. GRIMM, *Authenticating Digital Evidence*, in *GP Solo Magazine – American Bar Association*, 2014, 31, p. 49; P.W. GRIMM – D.J. CAPRA – G.P. JOSEPH, *Authenticating Digital Evidence*, in *Baylor Law Review*, 2017, p. 1 ss.

[26] *Shea c. Sati Uniti*, 167 S.W.3d 98 (Tex. Ct. App. 2005).

[27] In questo senso, v., ad es., F. BUENO DE MATA, *Prueba electrónica y proceso 2.0*, Valencia, 2014, p. 275; S. PEREIRA PUIGVERT, *De vuelta con la aportación y valoración de la prueba electrónica de Whatsapp y su interpretación acorde con el contexto y el testimonio de la denunciante. Comentario de la Sentencia del Tribunal Supremo (Sala de lo Penal) 920/2021, de 24 de noviembre*, in *La Ley Probática*, 2022, 7, par. 1, nt. 6.

tecnologia", si giunge financo ad affermare che, a fronte della minore specializzazione richiesta al singolo individuo, le prove analogiche sarebbero più agevolmente manipolabili e falsificabili rispetto a quelle elettroniche[28]. In definitiva, «*si bien es cierto que la prueba tecnològica es alterable, tambièn puede modificarse cualcquier documento impreso tradicional, o la declaraciòn de un testigo*»[29].

4. "*All evidence is equal, but some is more equal than others*": l'ingresso della *social network evidence* nel processo penale statunitense

A fronte di tale quadro, non era difficile immaginare che le problematiche sorte con riguardo alla prova elettronica si sarebbero riproposte pure con riferimento alla *social network evidence*. Non è raro, in effetti, imbattersi in affermazioni tanto perentorie quanto plasticamente rappresentative dell'assoluta dirompenza di questo fenomeno: «s*ocial media evidence is the new frontier of criminal proceedings and it raises unique legal challenges, inluding iddues of admissibility*»[30] e, ancora, «*the authentication of social media evidence has become a prevalent issue in litigation today, creating much confusion and disarray for attorneys and judges*»[31].

L'avvento di un nuovo "tipo probatorio" ha riacceso il dibattito tra "conservatori" e "progressisti", ovvero tra chi ritiene che l'attuale *standard*, spiccatamente permissivo (*threshold preliminary standard*), di autenticazione delle prove previsto dalle FRE sia adeguato a garantire le esigenze sottese al giudizio di ammissibilità e coloro che, per contro, sottolineano l'urgenza di una modifica normativa o, quantomeno di una chiara e rigorosa presa di posizione da parte della giurisprudenza.

I primi, in particolare, sembrano muovere dall'idea per cui l'applicazione di uno *standard* più elevato rispetto a quello attuale rischierebbe di esclude dal processo prove preziose, rispetto alle quali – si sostiene – il vero giudizio di affidabilità, una volta ammesse, dovrebbe essere compiuto dalla giuria a seguito dell'esame incrociato delle parti, nel quale potrà essere saggiata, in contraddittorio, l'effettiva genuinità o meno del materiale prodotto in giudizio[32].

A questo filone di pensiero si oppongono coloro che cercano di valorizzare la natura estremamente volatile e manipolabile delle informazioni ricavate dai *social network* (come,

---

[28] O. FUENTES SORIANO, *La impugnaciòn de la prueba digital*, in AA.VV., *Tendencias actuales del Derecho Procesal*, Valencia, 2019, p. 284. Concorde P. ARRABAL PLATERO, *La prueba tecnològica: aportaciòn, pràctica y valoraciòn*, Valencia, 2020, p. 45.

[29] P. ARRABAL PLATERO, *La prueba tecnològica*, cit., p. 45, la quale soggiunge come «*no se trata, por tanto, de un problema nuevo necesitado de soluciones originales o singulares […] existen garantìas suficientes en el proceso para la expulsiòn de quellas* [*pruebas*] *que estiviese adulteradas*» (338). Sembra adottare questa visione, nel panorama nazionale, M. CAIANIELLO, *L'ammissione della prova scientifica nel processo penale italiano*, in G. Canzio – L. Lupária (a cura di), *Prova scientifica e processo penale*, Milano, 2022, p. 192-195.

[30] J.P. MURPHY – A. FONTECILLA, *Social Media Evidence in Government Investigations and Criminal Proceedings*, cit., p. 11.

[31] P.W. GRIMM – L. BERGSTROM – M.M. O'TOOLE-LOUTERIO, *Authentication of Social Media Evidence*, in *American Journal of Trial Advocacy*, 2013, p. 433.

[32] Per questa opinione, v., ad es., B.M. DEMOCKO, *Social Media and the Rules on Authentication*, in *University of Toledo Law Review*, 2012, p. 402.

ad esempio, gli *user-generated contents*); caratteristiche, queste, che giustificherebbero un innalzamento dello *standard* di ammissibilità[33].

Il dibattito dottrinale e giurisprudenziale, lungi dall'essere esaurito, è stato portato all'attenzione del *Federal Rules of Evidence Advisory Committe* che, nel 2014, si è pronunciato sulla proposta di modifica della Rule 901 volta a includere nel dettato normativo regole *ad hoc* per l'autenticazione delle prove elettroniche e, in particolare, di quelle estrapolate dai *social network*[34]. A seguito di un'approfondita analisi, il Comitato ha rigettato la richiesta, sottolineando come l'attuale regolamentazione risulti sufficientemente ampia e flessibile da poter governare anche questa nuovo tipo probatorio. L'introduzione di un regime specifico, inoltre, si rivelerebbe – ad avviso del Comitato – alquanto problematica, dal momento che non sarebbe agevole individuare nel dettaglio le modalità di autenticazione richieste per le prove a contenuto tecnologico. Anche laddove si riuscisse in una tale operazione, peraltro, «*such rules would probably have to be constantly amended to keep up with technology*», rendendo così vano ogni tentativo di tipizzazione.

4.1 Il cd. *Maryland Approach*

L'approccio giurisprudenziale più rigoroso e scettico rispetto all'ammissibilità delle informazioni ricavate dai *social network* è stato manifestato per la prima volta nel caso *Griffin c. Stati Uniti*[35].

Per comprendere meglio il *dictum* enunciato dalla Corte di Appello del Maryland è utile prendere l'abbrivio da una sommaria enunciazione dei fatti oggetto di causa.

Nel procedimento per omicidio a carico del Sig. Griffin, il *prosecutor* aveva richiesto l'ammissione di una stampa (uno *screenshot*) di un profilo *MySpace* (un *social network* ampiamente diffuso in quegli anni) asseritamente riferibile alla fidanzata dell'imputato (la Sig.ra Barber), al fine di dimostrare l'avvenuta subornazione di alcuni testimoni dell'accusa. Dal documento prodotto in giudizio era possibile ricavare il nominativo dell'utente (trattavasi, invero, di un *nickname*: «*Sistahouljah*»), la sua data di nascita e una foto che rappresentava il Sig. Griffin con la propria fidanzata. Ad avviso del pubblico ministero, questi elementi muovevano a favore della riconducibilità del profilo in capo alla compagna dell'imputato. A tali conclusioni si opponeva, però, la difesa, sostenendo che le circostanze addotte dall'organo d'accusa non fossero sufficienti per dimostrare l'autenticità del documento, ovverosia la ragionevole convinzione di un collegamento tra il profilo *social* e la Sig.ra Barber.

---

[33] Si veda, in tal senso, C. MILLER, *The Social Medium: Why the Authenticantion Bar Should Be Raised for Social Media Evidence*, in *Template Law Review Online*, 2014, p. 1 ss.; S. CARLSON, *When is a Tweet Not an Admissible Tweet? Closing the Authentication Gap in the Federal Rules of Evidence*, in *University of Pennsylvania Law Review*, 2016, p. 1060. In giurisprudenza, cfr. *Griffin c. Stati Uniti*, 419 Md. 343, 19 A.3d 415 (2011); *Parker c. Stati Uniti*, 85 A.3d 682, 685-86 (Del. 2014); *Sublet c. Stati Uniti*, 113 A.3d 695, 712 (Md. 2015).

[34] ADVISORY COMMITTED ON EVIDENCE RULES, *Minutes of the Meeting of October 24*, 24 ottobre 2014, p. 191 ss.

[35] *Griffin c. Stati Uniti*, cit. Per un commento alla pronuncia, si rinvia a B.W. HOGAN, *Griffin v. State: Setting the Bar Too High for Authenticating Social Media Evidence*, in *Maryland Law Review*, 2012, p. 61 ss.

Nel ribaltare la pronuncia di primo grado che aveva ritenuto ammissibile la stampa della pagina *MySpace*, la *Maryland Court of Special Appeals* ha adottato un approccio, come anticipato, destinato "a fare scuola".

L'*iter* argomentativo accolto dai giudici muove da un assunto ben preciso: il rischio di potenziale manomissione o falsificazione della *social network evidence* pone «*significant challenges*» sul versante dell'autenticazione, specialmente con riguardo al settore dei *site printouts*. Ad avviso dei giudicanti, infatti, chiunque potrebbe creare un *account* fittizio, mascherarsi *online* sotto falso nome, manipolare una stampa di una pagina *web* o cancellare dati e informazioni presenti in una *chat*. È per tale ragione, dunque, che il timore per una possibile alterazione della prova *social* appare assai più concreto di quanto possa prospettarsi con riferimento a qualunque altro mezzo probatorio analogico. Applicando tali principi al caso di specie, la Corte ha ritenuto che gli elementi addotti dal pubblico ministero non fossero «*distinctive characteristic*» sufficienti per provare la riferibilità del *post* – e, ancor prima dell'*account* – al presunto autore.

Il paradigma interpretativo fatto proprio dai giudici del Maryland si riverbera direttamente sul versante dell'*onus probandi*: chi intende produrre in giudizio una prova estrapolata da un *social network* deve dimostrare l'autenticità del suo contenuto. La mera possibilità che il *bit* digitale possa essere stato creato da una persona diversa rispetto a quella cui è putativamente attribuito – anche in assenza di indizi circostanziali che dimostrino tale evenienza – è sufficiente per affermare, in via presuntiva, la non autenticità della prova[36]. In assenza di una dimostrazione negativa della non alterazione, dunque, la *social network evidence* non può trovare cittadinanza nel processo penale.

La pronuncia in esame, però, non si limita a enucleare una nuova regola giudiziale di apprezzamento della genuinità dei dati ricavati dalle piatteforme, bensì suggerisce alcune possibili modalità di autenticazione di tali informazioni[37].

Il riferimento corre, *in primis*, a quello che la stessa Corte definisce «*the first, and perhaps most obvious method*», cioè la dichiarazione testimoniale proveniente dal presunto autore della prova *social* (scritto, immagine, video, etc.).

In aggiunta, dovrebbe disporsi il sequestro e la perquisizione del dispositivo elettronico asseritamente utilizzato per la creazione del *bit* digitale del quale si richiede l'ammissione, sottoponendo lo stesso a un esame di *computer* o *mobile forensics*. A tal proposito, però, sia lecito esprimere qualche perplessità. È evidente, infatti, che il presunto autore del *post* o del messaggio potrebbe aver creato il proprio *account* da un *device* riferibile a terzi ovvero presente in luoghi (come, ad esempio, un *internet-point*) che non ne consentono l'identificazione. Peraltro, anche laddove si dimostrasse che quel determinato dispositivo in uso all'indagato (o al terzo comunque coinvolto nel processo) è stato effettivamente utilizzato per creare l'*account* nel quale è stato rinvenuto il materiale probatorio, ciò non

[36] P.W. GRIMM – L. BERGSTROM – M.M. O'TOOLE-LOUTERIO, *Authentication of Social Media Evidence*, cit., p. 455.

[37] In dottrina, in realtà, si è osservato come il catalogo previsto alla *Rule* 901(b) non rappresenti un *numerus clausus*, cosicché i criteri enunciati dalla Corte nel caso *Griffin*, ancorché teoricamente condivisibili, non impongono necessariamente una rimodulazione normativa delle attuali regole in tema di autenticazione (B.W. HOGAN, *Griffin v. State: Setting the Bar Too High for Authenticating Social Media Evidence*, cit., p. 85).

significa che il suo (apparente) titolare ne sia anche l'autore. In altre parole, quello che occorre sottolineare – e che, invece, non sembra essere stato colto appieno dalla pronuncia in esame – è l'inconsistenza del parallelismo tra la titolarità/disponibilità del *device* o dell'*account* e la paternità della prova *social* da esso ricavata[38].

Infine, laddove i dati di interesse siano stati conservati dal *provider*, occorrerebbe rivolgersi direttamente a quest'ultimo per ottenere la loro *disclosure*.

Nonostante la *dissenting opinion* manifestata nel caso di specie dal giudice Harrel[39] – richiamata a sostegno dell'opposto indirizzo giurisprudenziale sviluppatosi nello Stato del Texas, del quale si darà conto a breve[40] –, l'approccio restrittivo fatto proprio dalla Corte ha avuto seguito in ulteriori pronunce. Tra queste[41], meritano di essere espressamente menzionati i casi *Stati Uniti c. Sublet*[42], *People c. Backley*[43] e *Stati Uniti c. Eleck*[44].

Quanto al primo, la *Appeal Court* del Maryland – confermando il *dictum* espresso dai giudici di prime cure – ha sottolineato nuovamente come la fase di autenticazione delle prove estratte dalle piattaforme sia caratterizzata da ampi margini di incertezza legati alla facile alterabilità e manipolabilità dei dati e dall'estrema difficoltà di riuscire a individuare la paternità delle dichiarazioni, delle immagini o dei video in esse contenuti. Al netto della soluzione accolta nel caso di specie[45], la Corte si sofferma profusamente sulle ragioni a sostegno della necessità di una revisione normativa della *Rule* 904, riconoscendo, ad esempio, la maggiore difficoltà nel riuscire a provare la paternità di un dato digitale rispetto a un documento cartaceo, con riguardo al quale un esame calligrafico sarebbe in grado di sciogliere (quasi) ogni dubbio.

Di estremo interesse – specie, come si vedrà, nella prospettiva italiana – si rivela la pronuncia adottata dalla Corte di appello della California (*People c. Backley*), nella quale i giudici, dopo aver lapidariamente affermato che «*anyone can put anything on the Internet*», sottolineano come l'analisi eseguita da un *expert witness* sia sovente necessaria per autenticare le prove ricavate dalle piattaforme digitali, dal momento che, come noto, nell'era dell'*high-tech* non occorrono abilità sopraffine per modificare o alterare un dato informatico.

---

[38] Su tale aspetto, v. le condivisibili considerazioni di I.P. ROBBINS, *Writings on the Wall: The Need for an Autorship-Center Approach to the Autentication of Social-Networking Evidence*, in *Minnesota Journal of Law, Science and Technology*, 2012, p. 2 ss.

[39] Sulla quale v., *amplius*, R.W. FOX, *The Return of "Vodoo Information": A Call to Resist a Heightened Authentication Standard for Evidence Derived From Social Networking Websites*, in *Catholic University Law Review*, 2013, p. 197 ss., spec., p. 216 ss.

[40] Cfr. *infra*.

[41] *Commonwealth c. Wallick*, No. CP-67-CR-5884-2010 (Pa. Ct. Com. Pl. Oct. 2011), nella quale si afferma che la mera presenza dell'immagine o del nome di un soggetto nella pagina di *MySpace* non è sufficiente per autenticarne la genuinità; *Commonwealth c. Williams*, 926 N.E.2d 1162 (Mass. 2010).

[42] *Sublet c. Stati Uniti*, cit. Per un approfondito commento, cfr. E.A. FLANAGAN, *#Guilty: Sublet v. State and the Authentication of Social Media Evidence in Criminal Proceedings*, in *Villanova Law Review*, 2016, p. 287 ss.

[43] *People c. Backley*, 110 Cal. Rptr. 3d 362 (Ct. App. 2010).

[44] *Stati Uniti c. Eleck*, 23 A.3d 818, 821-25 (Conn. App. Ct. 2011).

[45] L'imputato, pur confermando la paternità dell'*account* dal quale erano stati inviati i messaggi incriminati, disconosceva di esserne l'autore, sostenendo di aver condiviso il nome utente e la *password* con persone terze. La Corte ha accolto l'argomentazione difensiva reputando inammissibile la prova presentata dal *prosecutor*.

Altrettanto significativo appare, infine, il *dictum* espresso dalla Corte Suprema del Connecticut (*Stati Uniti c. Eleck*), nella parte in cui vengono messe in discussione una serie di inferenze e massime di esperienza che nella realtà digitale non sembrano poter trovare applicazione. Con specifico riferimento al problema della paternità dei *post* e dei messaggi inviati tramite applicativi di *real-time conversation*, i giudici sottolineano come la semplice dimostrazione della loro provenienza da uno specifico *account* non sia sufficiente, in assenza di «ulteriori e stringenti indizi», per fondare un giudizio positivo di genuinità della prova. Difatti – si sostiene – pure nel caso in cui le credenziali di accesso non siano divulgate a terzi, permane comunque un rischio elevato che altri individui possano utilizzare il *device* senza il consenso del legittimo titolare[46].

4.2 Il cd. *Texas Approach*

A fronte di una presa di posizione particolarmente rigorosa sviluppatasi nelle Corti del Maryland – e, come visto, diffusasi anche in altri ordinamenti federali –, non sono mancati atteggiamenti più indulgenti e lassisti, come quello manifestato, *in primis*, nella fondamentale pronuncia *Tienda c. Stati Uniti*[47].

Pure in questa circostanza, la fattispecie concreta riguardava un caso in cui il pubblico ministero aveva richiesto l'ammissione delle fotografie di alcune pagine del *social network MySpace* presumibilmente riferibili all'imputato. Il tribunale di prima istanza – con una decisione poi confermata dalla *Court of Criminal Appeal* dello Stato del Texas – accoglieva la richiesta, ritenendo provata l'autenticità delle stampe alla luce dei numerosi indizi circostanziali («*ample circumstantial evidence*») apportati dall'organo d'accusa, dai quali era stato possibile dedurre la riferibilità all'imputato dell'*account*, dei *post* e dei messaggi *ivi* contenuti.

Facendo leva sull'applicazione della regola di autenticazione tipizzata nella *Rule* 901(b)(4), i giudici hanno affermato che chiunque voglia introdurre in giudizio un dato ricavato dalle piattaforme digitali debba addurre elementi o circostanze – anche mediante i metodi indicati alla *Rule* 901(b) – che siano sufficienti a convincere un "giudice ragionevole" della loro autenticità. Secondo tale indirizzo esegetico, la prova della genuinità del dato è rimessa, in buona sostanza, a un ragionamento indiziario, nell'ambito del quale il proponente è chiamato a individuare una serie di elementi dotati di rilevanza induttiva rispetto al fatto da provare.

Se la parte riesce a raggiungere lo *standard* richiesto, è onere di colui che si oppone all'autenticità dimostrare la falsità, la manipolazione o l'alterazione del predetto contenuto. A differenza dell'esegesi accolta dai giudici del Maryland, pertanto, il *burder of production*

[46] Si pensi, ad esempio, al caso – tutt'altro che remoto – in cui l'utente abbia lasciato collegato (loggato) il proprio profilo nel suo dispositivo, con conseguente possibilità di essere utilizzato da terzi o, ancora, all'ipotesi nella quale «*password and website security are subject to comprimise by hackers*» (*Stati Uniti c. Eleck*, cit.). Cfr. anche E.A. FLANAGAN, *#Guilty: Sublet v. State and the Authentication of Social Media Evidence in Criminal Proceedings*, cit., p. 301 ss.

[47] *Tienda c. Stati Uniti*, 358 S.W.3d 633, 641-42 (Tex. Crim. App. 2012). Nello stesso senso, v. *Stati Uniti c. Assi*, No. 1 CA-CR 10-0900, 2012 WL 3580488 (Ariz. Ct. App. Aug. 21, 2012).

(l'onere di produzione delle prove) finisce per gravare sul soggetto che intende contestare la genuinità del dato, il quale sarà chiamato a dimostrarne la manipolazione o l'alterazione.

5. Manipolazione digitale e *social network platforms*: l'incursione del *deepfake* nelle aule di giustizia

Dal breve *excursus* svolto fino a questo punto sembra emergere una netta contrapposizione tra due diverse scuole di pensiero. Il terreno di scontro sul quale dottrina e giurisprudenza sono chiamate a confrontarsi è sufficientemente chiaro: il potenziale di falsificazione proprio delle *new evidence* (si legga, la *social network evidence*) giustifica o meno un innalzamento dell'attuale *standard* di autenticazione nella materia in analisi?

Per dare conto dell'estrema pregnanza di tale dibattito, può essere interessante volgere brevemente lo sguardo a un altro fenomeno contiguo a quello fin qui esaminato. Il riferimento è al cd. *deepfake*, cioè «un sistema di IA che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona»[48].

Dal punto di vista della scienza linguistica, la locuzione *deepfake* è il frutto della "composizione" tra due parole: *deep learning* e *fake*. Se, com'è ormai noto, quest'ultima espressione allude a quel fenomeno comunemente denominato *fake news*, ovverosia la diffusione di notizie in tutto o in parte non corrispondenti al vero attraverso il *web* o le tecnologie digitali di comunicazione (i *social network*)[49], la prima, al contrario, risulta, perlomeno sotto il profilo tecnico-informatico, assai più complessa. In via del tutto approssimativa, è possibile definire tale concetto come una sottocategoria di "apprendimento automatizzato" costituita da *software* che, elaborando informazioni in *input* attraverso le interazioni tra reti neurali e sfruttando un metodo di programmazione computazionale, sono in grado di imitare il funzionamento dei meccanismi basici del celebro umano[50].

Sfruttando l'innovazione tecnologica conseguente alla diffusione di queste specifiche categorie di IA, gli informatici[51] hanno sviluppato un modello peculiare di *deep learning* che rappresenta l'attuale base tecnologica per la creazione dei *deepfakes*. Si allude alle cd. *Generative Adversarial Networks* (GANs), ovverosia "reti generative avversarie": una prima struttura, detta Generatore, riceve ed elabora dati in *input* al fine di produrre campioni

[48] È questa la definizione offerta dall'art. 52, comma 3 della Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale, 21 aprile 2021. In termini non dissimili si esprime pure il *report* redatto dalla *Scientific Foresight Unit* (STOA) dell'*European Parliamentary Research Service* del giugno 2021, nel quale il *deepfake* viene definito come «*manipulated or synthetic audio or visual media that seem authentic, and which feature people that appear to say or do something they have never said or done, produced using artificial intelligence techniques, including machine learning and deep learning*».

[49] Cfr., per tutti, T. GUERINI, Fake news *e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Torino, 2020.

[50] A differenza dell'informatica tradizionale, nell'ambito della quale le macchine operavano in base a regole e codici prescelti dagli esseri umani, la categoria della *machine learning* (di cui, come detto, il *deep learning* costituisce un sotto-insieme) consente al programmatore di dar vita a un sistema nel quale l'artefatto è in grado di apprendere e svolgere una funzione in assenza di istruzioni esplicite.

[51] Lo studio cui si allude è quello prodotto da un gruppo di ricercatori del Dipartimento di informatica dell'Università di Montreal: I.J. GOODFELLOW *et al*., *Generative Adversarial Networks*, in *arXiv*, 2014.

verosimili di video, immagini o audio; una seconda, conosciuta come Discriminatore, cerca di differenziare i campioni generati da quelli reali. Il sistema, così per come concepito, è in grado di fornire continuamente un *feedback* a sé stesso, valutando l'autenticità delle informazioni prodotte dal Generatore e fornendo costantemente *input* per migliorare la qualità del risultato generato dal primo sistema di IA, fino a quando il *computer* stesso non è più in grado di determinare la differenza tra l'immagine "in uscita" e il *file* originale[52].

Sul versante giuridico, la prima trattazione di carattere sistematico degli aspetti correlati alla diffusione di questa nuova forma di manipolazione audiovisiva può essere datata 1° febbraio 2019, allorquando la *Maryland Law Review* ha riunito alcuni studiosi del settore in un simposio dal titolo «*Truth Decay: Deep Fakes and the Implications for Privacy, National Security, and Democracy*». Si è trattato di un vero e proprio spartiacque, tanto che, ad oggi, punto di riferimento per l'analisi della materia è lo studio prodotto dai due principali relatori di quella conferenza, i quali hanno messo in evidenza come le conseguenze di tale fenomeno possano spaziare dal settore sociale a quello psicologico, passando per quello giuridico, fino a intaccare quello macroeconomico[53].

Ancorché gli studi relativi all'impiego di questa nuova tecnologia nell'ambito del processo penale siano quantitativamente limitati[54], le possibili interazioni tra rito criminale e *deepfake* risultano tutt'altro che fantascientifiche o futuristiche. Per quel che più interessa in questa sede, non può dubitarsi del fatto che tra le informazioni acquisibili nei *social network* vi siano anche possibili video oggetto di falsificazione mediante *deepfake technologies*. Anzi, i SNS, lo si è detto, costituiscono la sede privilegiata nella quale questa tipologia di "inganno digitale" può esplicare maggiormente i suoi effetti perversi. Com'è stato osservato, infatti, «i materiali [contenuti nei *social network*] sono spesso aperti al pubblico e chiunque abbia una conoscenza pratica della tecnologia può usarli per creare praticamente tutto ciò che vuole»[55].

---

[52] Il confronto interattivo tra i due algoritmi è "croce e delizia" dei *software deepfakes*: man mano che il Discriminatore migliora nell'individuazione dei falsi, esso fornisce un *feedback* al Generatore che, a sua volta, impara dai propri errori e produce risultati sempre più realistici. In questo circolo virtuoso, il Generatore cercherà di "ingannare" il Discriminatore, tentando di produrre campioni che quest'ultimo classificherà erroneamente come reali. Le potenzialità di questa nuova forma di "tecnologia distruttiva" sono assai numerose. Si considerino, solo per fare alcuni esempi: a) la cd. *image-to-image translation*, ovverosia la possibilità di alterare completamente il contesto di un'immagine (ad esempio, trasformando una pistola in un coltello); b) la cd. *sketch-to-image translation* e, cioè, l'alterazione dei colori all'interno di un'immagine; c) l'alterazione degli attributi dei visi delle persone attraverso *i*) la sintesi *ex novo* di un volto (*entire face synthesis*), *ii*) la modifica dell'espressione facciale (*expression swap* o *reenactment* del volto), *iii*) la sostituzione di un volto di una persona con il volto di un'altra (*identity swap*) e, ancora, *iv*) la manipolazione degli attributi del viso, come ad esempio, il colore dei capelli (*attribute manipulation*).

[53] D.K. CITRON – R. CHESNEY, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, in *California Law Review*, 2019, p. 1753 ss.

[54] Sia consentito il rinvio ad A. MALACARNE, "*Profundamente falso" y "profundamente incierto": el deepfake como* automated evidence *en el proceso penal. Consideraciones generales*, in *Revista General de Derecho procesal*, 2023, 60, p. 1 ss.

[55] E. CALDERA, *Reject the Evidence of Your Eyes and Ears: Deepfakes and the Law of Virtual Replicants*, in *Seton Hall Law Review*, 2019, p. 179 (trad. nostra). Nel marzo 2021, ad esempio, una donna della Pennsylvania è stata arrestata ed accusata di molestie per aver asseritamente creato un video *deepfake* nel quale apparivano alcune compagne di squadra della figlia in stato di ubriachezza. La donna, conosciuta pubblicante come «*mother cheerleader deepfake*», ha negato fin dall'inizio ogni suo coinvolgimento nella vicenda. Il Procuratore, tuttavia, ha ritenuto di procedere comunque nei suoi confronti. Sennonché, a distanza di tempo,

Ebbene, pure in tale contesto la principale *quaestio iuris* che si va affacciando nel recente dibattito dottrinale d'oltreoceano attiene al profilo dell'autenticità della prova. In breve: il potenziale di falsificazione dei video digitali giustifica una modifica dei criteri e delle regole che disciplinano l'attività delle parti e del giudice nell'arco del procedimento probatorio?

Alcuni commentatori sostengono che la mera possibilità di imbattersi in un video oggetto di GANs *manipulation*, ancorché niente affatto ridotta, non richieda comunque un livello elevato di autenticazione, posto che le attuali regole processuali risultano adeguate ad affrontare tale fenomeno[56]: «*deepfake technology is new, but it does not present novel challenges*»[57]. Si è sottolineato, in effetti, come pure in passato le "nuove" tecnologie (si pensi, ad esempio, al DNA) abbiano posto sul tavolo questioni problematiche in termini di autenticazione e valutazione del dato acquisito in giudizio e come, tuttavia, in queste situazioni, alla fine, il sistema processuale abbia risposto al meglio a tali sfide.

Al netto della condivisibilità di tale ultima affermazione (sulla quale, in realtà, pare potersi dubitare[58]), non v'è chi non veda come i *deefakes*, per progettazione e potenzialità di ingannano dello spettatore, sollevino domande esistenziali sulla realtà a un livello profondo e metafisico tale da rendere le tematiche in questione assai più complesse rispetto al passato. Per tali motivi, altra dottrina ha messo in guardia dal rischio che l'emergere di una tecnologia di tipo "auto-generativo", capace di sfruttare le potenzialità offerte dall'apprendimento automatico, possa produrre immagini, video e audio alterati, più realistici e più difficili da smascherare rispetto al passato[59]. Se ne è dedotto, sul piano processuale, che nessuna delle regole federali in materia probatoria può dirsi sufficiente, allo stato attuale, per affrontare le sfide significative poste dalla tecnologia *deepfake*: «*evidentiary standards need to evolve to accommodate our changing world*»[60].

6. Osservazioni di sintesi

L'approccio delle Corti e della dottrina d'oltreoceano alla *social network evidence* – e alla *deepfake evidence* – appare tutt'altro che uniforme. La ragione alla base dei differenti canoni interpretativi adottati dai giudici federali sembra potersi individuare nel diverso punto di osservazione del fenomeno *de quo*.

---

lo stesso prosecutor ha annunciato di non voler proseguire nell'esercizio dell'azione penale con riguardo all'accusa di manipolazione, svelando in pubblica udienza che l'ufficiale di polizia giudiziaria coinvolto nelle indagini aveva concluso per la veridicità del video basandosi esclusivamente su una valutazione «a occhio nudo» (*https://www.washingtonpost.com/technology/2021/05/14/deepfake-cheer-mom-claims-dropped/*).

[56] Per questa lettura, v., ad es., R. PFEFFERKORN, *"Deepfakes" in the Courtroom*, in *Boston University Public Interest Law Journal*, 2020, p. 267.

[57] M. FEENEY, *Deepfake Laws Risk Creating More Problems Than They Solve*, in *Regulatory Transparency Project of the Federalist Society*, 1° marzo 2021, p. 1.

[58] Il tema, come noto, è tutt'ora al centro di un acceso dibattito. Cfr., per una panoramica delle principali questioni sul tappeto, C. CONTI, *La prova scientifica alle soglie dei vent'anni dalla sentenza Franzese: vette e vertigini in epoca di pandemia*, in *Sist. pen.*, 9 febbraio 2021.

[59] Cfr. M.H. MARAS – A. ALEXANDROU, *Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos*, in *The International Journal of Evidence & Proof*, 2019, p. 255 ss.

[60] J.P. LAMONAGA, *A Break From Reality: Modernizing Authentication Standards for Digital Video Evidence in the Era of Deepfakes*, in *American University Law Review*, 2020, p. 1988. Nello stesso senso, v. C. BREEN, *Silent No More: How Deepfakes Will Force Courts to Reconsider Video Admission Standards*, in *The Journal of High Technology Law*, 1° giugno 2021, p. 162.

Nelle pronunce afferenti al cd. *Maryland Approach*, le Corti muovono dall'idea secondo cui le prove raccolte nelle piattaforme di *sharing* dovrebbero essere sottoposte a un vaglio di ammissibilità più stringente rispetto a quello stabilito per le prove tradizionali, in ragione della loro spiccata volatilità e manipolabilità. In questa prospettiva, vi è chi propende per una radicale modifica dell'attuale dettato normativo (si legga, delle FRE), ritenuto inadeguato nell'attuale contesto storico e chi, invece, suggerisce, *de iure condito*, di ricorrere a un'esegesi restrittiva dello *standard* di autenticazione, allocando l'onere della prova in capo a colui che intende produrre in giudizio il *bit* digitale. A quest'ultimo proposito, si è potuto osservare, altresì, come alcune pronunce giurisprudenziali si soffermino in maniera approfondita sulla necessità di un'analisi tecnico-informatica del *device* – il contenitore delle informazioni presenti nei *social network* – che assurgerebbe a "prova regina" per saggiare la genuinità del materiale prodotto in giudizio.

In questo contesto, grava sul proponente l'onere di provare che l'informazione estrapolata dai *social network* risulta autentica, cioè idonea a rappresentare quanto in essa contenuto. In ragione delle caratteristiche del *bit* informatico, però, lo *standard* richiesto non può essere quello tradizionalmente indicato nella *Rule* 901 e, in particolare, l'impiego del criterio delle *distinctive circumstances* o del *corroboration approach*[61]. Ciò che occorre – nel solco dell'esegesi in esame – è, invece, un livello di autenticazione più elevato, il cui obiettivo sia quello di contrastare l'ingresso nel processo della "*junk technology*".

In una dimensione diametralmente opposta si collocano, per converso, quelle sentenze che fanno capo al cd. *Texas Approach*, dalla lettura delle quali emerge una chiara "scelta di campo": *social network evidence* e prove analogiche pongono gli stessi problemi in termini di autenticità e genuinità del dato. D'altro canto – viene osservato – pure un semplice documento cartaceo può essere manipolato o firmato e inoltrato tramite servizio postale da un soggetto che non corrisponde al reale mittente. Di conseguenza, nessuna valida ragione vi sarebbe a sostegno della necessità di condurre un giudizio di autenticazione delle prove ricavate dai *social network* con uno *standard* più elevato rispetto a quello attualmente previsto dalla legge[62]. Se ne ricava, sul versante dell'*onus probandi*, la necessità che il proponente dimostri, alla luce di un parametro assai indulgente e permissivo (*rectius*, quello di cui alla *Rule* 901, così per come interpretata dall'attuale giurisprudenza), che quella prova possa essere ritenuta autentica da un "giurato ragionevole". Se ciò avviene, graverà sulla controparte contestare la genuinità del dato apportato in giudizio.

[61] *Stati Uniti c. Quintana*, 763 F. App'x 422 (6th Cir. 2019).

[62] Cfr. *Stati Uniti c. Green*, 75. 830 S.E.2d 711 (S.C. Ct. App. 2019); *Stati Uniti c. Farrad*, 895 F.3d 859, 879-80 (6th Cir. 2018); *Stati Uniti c. Hannah*, 151 A.3d 99, 106 (N.J. App. Div. 2016), ove si afferma che «*a tweet can be easily forged, but so can a letter or any other kind of writing" and declining to "create a new test for social media postings*».

CAPITOLO II

LA PROSPETTIVA ITALIANA

SOMMARIO: 1. Dalla "prassi" alla "regola": il cd. *screenshot* quale prova documentale 2.0. – 2. L'autenticità della *social network evidence*: brevi cenni alla cd. *captura de pantalla* nel sistema spagnolo. – 3. Lo "scatto fotografico" della pagina *social* nell'esperienza italiana. – 3.1 …in ipotesi di non contestazione. – 3.2 Nuove sfide in tema di genuinità del *bit* digitale: dall'inadeguatezza dei modelli di controllo *ex post* alle nuove forme di certificazione preventiva. – 4. L'accertamento della paternità dei contenuti presenti nelle piattaforme.

1. Dalla "prassi" alla "regola": il cd. *screenshot* quale prova documentale 2.0

Com'era prevedibile, il tema relativo alla disciplina processuale applicabile per l'ammissione delle prove ricavate dai *social network* non ha tardato a manifestarsi pure nell'ordinamento italiano. Se, come osservato, dottrina e giurisprudenza d'oltreoceano sono state le prime, nel panorama internazionale, a confrontarsi con simili problematiche, l'attenzione della letteratura nostrana per il fenomeno *de quo* è stata sollecitata dal formarsi di un indirizzo pretorio rispetto al quale i commentatori hanno espresso perlopiù vivaci critiche.

Più in dettaglio, nella prassi giudiziaria è sempre più frequente assistere ad attività processuali, realizzate tanto dall'accusa, quanto dalla difesa, consistenti nella produzione dibattimentale di "supporti cartacei" rappresentativi di elementi probatori ricavati dai *social network*[1]. Che si tratti di dati segreti (come, ad esempio, le conversazioni intrattenute attraverso le applicazioni di messaggistica istantanea), ovvero di dati pubblici (come nel caso di *post* pubblicati nella bacheca di *Facebook*), il cd. *screenshot* rappresenta ormai la modalità principale con la quale le parti apportano in giudizio il materiale processualmente rilevante raccolto in Rete. La locuzione di derivazione anglosassone, invalsa nel gergo comune, allude, come noto, alla realizzazione di un fermo-immagine, una sorta di "scatto fotografico istantaneo" della schermata di un dispositivo elettronico (*tablet* o *smartphone*). Si tratta, a ben vedere, di una modalità 2.0 dell'ormai superata fotografia dello schermo utilizzata agli inizi degli anni 2000, a seguito della diffusione dei primi modelli di cellulare con videocamera incorporata, per fissare quanto visualizzato sul *display* del *personal computer*.

Dal punto di vista della rappresentazione dei fatti *ivi* contenuti, lo *screenshot* consegna una raffigurazione indiretta di "terzo livello"[2]: *in primis*, l'apparato elettronico è chiamato a

[1] Più in generale, rilevava, già anni or sono, come il «*social network material*» sarebbe presto divenuto un «elemento di prova centrale nella aule di giustizia», L. LUPÁRIA, *Il sistema penale ai tempi dell'*Internet. *La figura del provider tra diritto e processo*, in Id (a cura di), Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, p. 9.

[2] Nello stesso senso, v. M. PITTIRUTI, *L'impiego processuale dei messaggi inviati mediante l'applicazione* Telegram *tra "scorciatoie" probatorie e massime di esperienza informatiche*, in *Dir. Internet*, 2020, p. 318; G. FIORELLI, *Lo* screenshot *quale prova documentale: regole acquisitive e garanzie di affidabilità*, in *ivi*, 2020, p. 507. Di una rappresentazione di «secondo livello» parla, invece, R. DEL COCO, *L'utilizzo probatorio dei dati* whatsapp *tra lacune normative e avanguardie giurisprudenziali*, in *Proc. pen. giust.*, 2018, p. 535.

elaborare e, in seguito, decifrare il *bit* espresso in valori numerici per renderlo comprensibile alla mente umana; *in secundis*, il *monitor* è sottoposto a un'istantanea che ne estrapola una porzione spazio-temporale; e, da ultimo, il fermo-immagine è consegnato al processo mendiate una stampa cartacea.

Orbene, l'impiego così diffuso di questo nuovo "veicolo probatorio" rappresenta, a ben riflettere, la risposta della prassi giudiziaria all'estrema volatilità dei dati informatici presenti nelle piattaforme di *sharing* e, talvolta, alla mancanza – per le ragioni più disparate, tra le quali, invero, debbono annoverarsi le ridotte capacità economiche dell'imputato – di strumenti tecnici più raffinati in grado di "scansionare" il dato. Questa circostanza, però, non deve affatto stupire. In un sistema processuale moderno nel quale il compendio probatorio è costituito, sempre più frequentemente, da materiale digitale formato al di fuori del procedimento penale e in un momento antecedente al suo avvio, i soggetti e le parti processuali (pubblica e private) hanno la necessità di cristallizzare il *bit* informatico nel momento stesso in cui esso viene immesso nella piattaforma. Il pericolo di una futura dispersione è talmente elevato da non lasciare margine di scelta: la manipolabilità delle *user-generated information* impone a colui che visualizzi un contenuto *online* (avente possibile rilevanza processuale) di acquisirlo all'istante.

In questo contesto, il *punctum dolens*, dal punto di vista processuale, attintene, innanzitutto, al corretto inquadramento probatorio di detta operazione.

Nonostante i dissensi manifestati da una parte della dottrina[3], l'esecuzione del "fermo immagine" sembra potersi tendenzialmente ricondurre nel *genus* della prova documentale di cui all'art. 234 c.p.p.[4]. Del resto, se l'obiettivo perseguito dalla parte è quello di cristallizzare un dato informatico, quale miglior modo che ricorrere a un mezzo di prova la cui più intima caratteristica è quella di rendere immanente e duraturo nel tempo qualcosa che, per sua natura, è sfuggente e transitorio?

La categoria *de qua*, è noto, rappresenta una *species* probatoria volutamente incompiuta e dai contorni alquanto sfumati. Sono ben conosciute le ragioni a sostengo di tale scelta legislativa: il progresso scoraggia dall'adottare una nozione stringente di documento, incentivando, all'opposto, l'accoglimento di un concetto elastico, malleabile e adattabile, capace di ricomprendere in sé ogni rappresentazione di «fatti, persone o cose» mediante «qualsiasi […] mezzo» che la tecnologia possa mettere a disposizione dell'essere umano[5].

Se, dunque, per documento – come ha efficacemente argomentato una parte della dottrina – si deve intendere una qualunque «cosa che incorpora segni» frutto del «risultato di un

[3] Si veda, ad es., M. PITTIRUTI, *L'impiego processuale dei messaggi inviati mediante l'applicazione* Telegram, cit., p. 318.

[4] Lo *screenshot*, in assenza di una stampa cartacea, dovrebbe essere qualificato alla stregua di un documento informatico. Concorde pure A. VELE, *Aspetti critici del documento probatorio "*screenshot*" e acquisito mediante il captatore informatico*, in *Arch. pen.* web, 8 marzo 2024, p. 3, il quale lo definisce come «l'immagine di una schermata o porzione di essa visibile su di un *display* di un dispositivo elettronico (*smartphone*, *tablet*, *pc*, *monitor*, televisione, etc.) acquisita tramite copia e salvata in possibili formati digitali diversi od appositi programmi».

[5] Sulla natura "aperta" del concetto di documento adottato dal legislatore dell'88 proprio al fine di rendere la norma adattabile allo sviluppo delle nuove tecnologie, v. L. KALB, *Il documento nel sistema probatorio*, Torino, 2000, p. 72.

lavoro umano, realizzato con l'impiego d'"apparati di rappresentazione" costituiti da tecniche più o meno sofisticate, di carattere analogico oppure digitale»[6], non si vede perché mai l'istantanea di uno schermo non possa rientrare a pieno titolo in detta categoria. Lo *screenshot* prodotto in giudizio, in questa prospettiva, costituisce una forma moderna di documento analogico, giacché la stampa del *file* digitale non fa altro che rendere visibili i *bit* presenti nel *social network* (*rectius*, il documento informatico[7]).

È certamente vero, lo si è detto, che lo *screenshot* simboleggia una sorta di "rappresentazione di terzo livello" del codice informatico *ivi* incorporato; come è altrettanto vero che questa caratteristica, lo si vedrà a breve, incide profondamente sul giudizio di autenticità del fatto incorporato. Eppure, ciò non sembra comunque sufficiente per escludere la "foto del *display*" dal novero delle prove documentali, dal momento che nell'art. 234 c.p.p., piaccia o meno, non è contenuto alcun riferimento esplicito a un qualche forma di certificazione della genuinità del dato rappresentato. In altre parole, ai fini della qualificazione in termini documentali, non è necessario che il supporto garantisca la non alterazione delle informazioni[8]. Ciò che rileva, invece, è l'astratta idoneità del metodo di incorporazione (analogico o digitale) di rappresentare «fatti, persone o cose».

In realtà, è forse superfluo – ma, comunque, opportuno – sottolineare che la conclusione alla quale si è pervenuti poc'anzi non possa estendersi anche alla realizzazione di *screenshot* quale modalità (elusiva) di documentazione di attività processuali da parte degli organi di indagine.

Dal punto di vista sistematico, infatti, la disciplina contenuta agli artt. 234 ss. c.p.p. – come enunciato, a chiare lettere, nella *Relazione al progetto preliminare* del nuovo codice[9] – può essere invocata solo qualora la cristallizzazione del fatto sia avvenuta "prima" e "al di fuori" dell'*iter* procedimentale ad opera di soggetti diversi dalle parti[10]. Di converso, qualora detta operazione sia il frutto di un'attività svolta dall'autorità procedente in pendenza di causa, la disciplina in tema di prove precostituite non può trovare applicazione. Alla luce di tale distinzione, pertanto, deve ritenersi preclusa alla polizia giudiziaria, che sia in grado di accedere alle piattaforme di *sharing* in uso all'indagato, la possibilità di realizzare uno *screenshot* della schermata del dispositivo e invocare l'ammissibilità del compendio probatorio ai sensi dell'art. 234 c.p.p. Diversamente opinando, il presidio della legalità probatoria sarebbe all'evidenza eluso: l'atto, in detta circostanza, è formato "nel corso" del procedimento e, di riflesso, deve soggiacere alle regole stabilite per l'acquisizione delle prove formate "nel" rito.

---

[6] F. ZACCHÈ, *La prova documentale*, Milano, 2012, p. 8 s.

[7] Ad analoga conclusione sembra giungere pure G. VACIAGO, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012, p. 3.

[8] In termini non dissimili, ancorché con riguardo, più in generale, al documento elettronico, v. F. ZACCHÈ, *La prova documentale*, cit., p. 36. In una differente prospettiva parrebbe collocarsi, invece, L. KALB, *Il documento nel sistema probatorio*, cit., p. 80.

[9] Relazioni al progetto preliminare e al testo definitivo del codice di procedura penale, GU n. 250 del 24-10-1988 - Suppl. Ordinario n. 93, p. 637.

[10] L. KALB, *Il documento nel sistema probatorio*, cit., p. 57; G. UBERTIS, *Variazioni sul tema dei documenti*, in *Cass. pen.*, 1992, p. 2516 ss.

2. L'autenticità della *social network evidence*: brevi cenni alla cd. *captura de pantalla* nel sistema spagnolo

L'aspetto più problematico e delicato che aleggia attorno all'impego processuale degli *screenshot* riguarda, come accennato, l'autenticità e la genuinità del dato digitale *ivi* rappresentato. Il rischio di manipolazione è, difatti, particolarmente elevato, dal momento che può avvenire, astrattamente, in tre diversi momenti: nella fase di esecuzione del fermo immagine (si pensi, all'impiego di applicazioni di *photo editing*); intervenendo a monte sulla genuinità del dato digitale, attraverso la modifica della cronologia dei messaggi; o, infine, generando *ex novo* informazioni (*chat*, fotografie, video, etc.) inesistenti nella realtà fenomenica.

A fronte di un rischio concreto di alterabilità dei dati, il legislatore del 2008, come si è più volte sottolineato, è intervenuto prescrivendo, a livello codicistico, l'adozione di una serie di garanzie atte ad assicurare che ispezioni, perquisizioni e sequestri siano realizzati in modo da garantire l'immodificabilità e l'inalterabilità dei *bit* informatici. Il *lawmaker*, però, non è stato altrettanto solerte con riguardo alla prova documentale, rispetto alla quale, *de iure condito*, nessuna disposizione normativa esige un qualche, neppur minimo, livello di tutela della genuinità del dato incorporato[11].

In realtà, è interessante osservare come tale disinteresse sia stato manifestato in altri ordinamenti, pure firmatari della Convenzione di Budapest sul *Cybercrime*. Ne è un chiaro esempio, il dibattito sviluppatosi tra i processualisti spagnoli, chiamati a confrontarsi, a fronte di un orientamento giurisprudenziale non sempre lineare, sulla validità delle fonti di prova tecnologiche introdotte in giudizio mediante un *pantallazo* (si legga, uno *screenshot*).

Le riflessioni della letteratura iberica si sono fatte via via più corpose a seguito del *leading case* rappresentato da una pronuncia del *Tribunal Supremo* (Sezione penale) del 19 maggio 2015, n. 300, che ha fornito una sorta di *vademecum* per la trattazione processuale dello *screenshot*. Nel caso di specie, la vittima introduceva in giudizio alcuni *pantallazos* o *capturas del pantalla* delle *chat* intercorse, nel *social network Tuenti*, tra la stessa e un compagno di scuola, nelle quali la ragazza confessava le violenze subite dal compagno della madre.

Ebbene, l'*iter* argomentando adottato dal giudice relatore muove da una premessa tanto perentoria, quanto condivisibile: la prova di una comunicazione realizzata attraverso una piattaforma digitale «*debe ser abordada con todas las cautelas*», giacché «*la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas*». L'anonimato e la volatilità che caratterizzano queste forme di comunicazione rendono non solo elevato il rischio di una manipolazione del contenuto di quanto *ivi* rappresentato, ma anche «*perfectamente posible*» che chiunque "modelli" *ex novo* una comunicazione in realtà mai avvenuta. In effetti, non occorre essere esperti informatici per eliminare parti di una conversazione o segmenti di un'immagine.

In ragione di tale rischio, il tribunale giunge ad affermare che, se la controparte *impugna* l'autenticità del fermo-immagine, mettendo in discussione la sua autenticità o l'integrità di

[11] F. ZACCHÈ, *La prova documentale*, cit., p. 31.

quanto in esso rappresentato, la parte che intende avvalersi del documento assume l'onere di provarne l'idoneità probatoria. Tale dimostrazione – ad avviso della Corte – deve essere fornita, ed è questo un passaggio fondamentale, attraverso «*la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido*».

La sentenza si fa apprezza specialmente per la presa d'atto del pericolo, tutt'altro che remoto, di una possibile alterazione dei dati digitali contenuti nella "fotocopia della schermata", nonché per la soluzione proposta onde evitare detta manipolazione. E, in effetti, nonostante alcune – ma, a dire il vero, isolate – pronunce di senso contrario nelle quali si è sostenuto che la mera possibilità di modificare dette informazioni è «*realmente remota y de notable dificultat tècnica*»[12], la giurisprudenza successiva sembra essersi allineata a tale *dictum*[13]. Particolarmente significativa, ai fini dello studio che si va conducendo, si rivela un arresto del 2017 nel quale i giudici hanno affermato che la richiesta di ammissione di uno *screenshot* raffigurante conversazioni *Whatsapp*, in assenza della messa a disposizione del dispositivo elettronico dal quale esso è stato ricavato, si rivela essere «*sumamente dèbil para probar que dichas conversacones tivieron lugar*»[14].

A fronte di tali arresti pretori, non stupisce che nella prassi giudiziaria iberica si vada sempre più diffondendo, tra gli operatori del diritto, una cultura processuale "dell'auto-certificazione preventiva". Con ciò, si allude alla tendenza di chi voglia introdurre in giudizio un *pantallazo* ricavato da un *social network* di accompagnare detto documento da una perizia o una trascrizione integrale che accerti l'affidabilità del suo contenuto e l'assenza di manipolazione. Questa prassi virtuosa sembra essere dovuta, almeno in parte, a un recente presa di posizione dei giudici lavoristi che, con riguardo all'ammissibilità del *pantalloazo*, vanno adottando parametri particolarmente stringenti. Oltre alla «*copia en papel de la impresión*», i le corti richiedono la trascrizione integrale della conversazione dalla quale esso è estratto, nonché – ed è questo il passaggio fondamentale – la certificazione di un esperto informatico che comprovi «*que la conversación se corresponde con el teléfono y con el número respectivos*»[15].

3. Lo "scatto fotografico" della pagina *social* nell'esperienza italiana

Uno sguardo, pur breve, al dibattito sviluppatosi nell'ordinamento iberico, risulta di grande utilità allorquando si intenda analizzare, *funditus*, la rilevanza del problema *de qua agitur* nel modello processuale italiano. A tal proposito, sembra opportuno esaminare

[12] AP Salamanca, Sez. I, 3 luglio 2017, n. 45. L'assunto è smentito, dal punto di vista informatico, dall'elevatissimo rischio di manipolazione dei messaggi scambiati attraverso l'applicazione *Whatsapp*. Cfr. L. RUBIO ALAMILLOS, *Vulnerabilidad en WhatsApp: falsificación de mensajes manipulando la base de datos*, al sito *https://peritoinformaticocolegiado.es/blog/vulnerabilidad-en-whatsapp-falsificacion-de-mensajes-manipulando-la-base-de-datos/, 29 settembre 2015*.

[13] Cfr., tra le molte, Tribunale Supremo spagnolo, 27 novembre 2015, n. 754; AP Barcellona, Sez. XX, 3 giugno 2016, n. 504; SAP La Rioja, Sez. I, 5 ottobre 2015, n. 111; SAP Sivilla, Sez. IV, 22 settembre 2017, n. 437. In precedenza, nello stesso seno, v. AP Huesca, Sez. I, 29 settembre 2014, n. 156.

[14] AP Burgos, Sez. III, 22 settembre 2017, n. 437.

[15] STSJ Galicia, 28 gennaio 2016, n. 556.

separatamente due ipotesi che, pur intimamente legate tra loro, impongono di svolgere riflessioni in parte differenti.

3.1 … in ipotesi di non contestazione

In primo luogo, v'è da chiedersi quale debba essere il contegno del giudice a fronte di un riconoscimento, esplicito o implicito, di autenticità dello *screenshot* ad opera di tutte le parti in causa. Detto altrimenti, *quid iuris* nel caso in cui nessuno contesti la genuinità del "fermo immagine"?

L'ipotesi in esame sembra potersi ricondurre, senza troppe difficoltà, nella categoria del cd. fatto pacifico, come tale non bisognoso di essere provato[16].

Il principale dubbio interpretativo, però, ruota attorno alla possibilità di attribuire alla volontà (ancorché unanime) delle parti – che nel modello accusatorio trova la sua massima espansione – una sorta di *potestas certificandi* della genuinità delle informazioni contenute nello *screenshot*. Occorre chiedersi, in altre parole, se il principio di non contestazione probatoria sia sufficiente per accreditare la genuinità del dato informatico rappresentato nel fermo-immagine.

Il quesito, è evidente, merita una risposta negativa. Del resto, pure qualora si tratti di acquisire la confessione dell'imputato, il giudice è libero di valutare, secondo il proprio apprezzamento, la genuinità della dichiarazione *contra se*. Qui, come altrove, le esigenze di tutela dell'affidabilità dell'accertamento, dipendenti dalla genuinità del dato informatico, ostano a un ingresso indiscriminato di qualsivoglia materiale probatorio.

3.2 Nuove sfide in tema di genuinità del *bit* digitale: dall'inadeguatezza dei modelli di controllo *ex post* alle nuove forme di certificazione preventiva

Quid iuris, invece, nel caso in cui l'acquisizione dello *screenshot* sia oggetto di contestazione ad opera della controparte?

È ben possibile – e accade non di rado– che venga messa in dubbio tanto la riconducibilità dell'*account* all'asserito autore del messaggio, quanto la genuinità del contenuto. Specialmente in quest'ultima ipotesi, occorre chiedersi se la riproduzione cartacea del *bit* digitale sia atta a dimostrare la realtà in esso rappresentata. Il quesito, è opportuno precisarlo, riguarda tanto il caso in cui lo *screenshot* venga prodotto dalla difesa, quanto nell'ipotesi in cui l'acquisizione sia richiesta dall'accusa: il tema dell'autenticità, difatti, si pone a prescindere dalla parte che intenda chiederne l'ammissione (imputato, pubblico ministero, parte civile)[17].

Con riguardo all'ipotesi presa in considerazione, dovrebbe ritenersi valido, in linea di massima, il principio secondo cui il soggetto che vuole introdurre nel giudizio una prova tecnologica (o un suo surrogato, come nel caso dello *screenshot*) è chiamato a corroborarne l'attendibilità e l'autenticità. Non si tratta, è bene sottolinearlo, di un'inversione dell'onere della prova, come tale inconciliabile con il principio cristallizzato all'art. 27, comma 2, Cost.

---

[16] P. TONINI – C. CONTI, *Il diritto delle prove penali*, Milano, 2014, p. 72.

[17] Concorde pure M. PITTIRUTI, *L'impiego processuale dei messaggi inviati mediante l'applicazione* Telegram, cit., p. 320.

È ben vero che nel rito penale l'innocenza è "presunta" e può essere superata solo laddove le prove addotte dall'accusa sono in grado di dimostrare la colpevolezza "oltre ogni ragionevole dubbio". Pur tuttavia, ciò non dispensa la parte dal dover avvalorare la genuinità del materiale informatico apportato nel processo, anche perché, com'è intuibile, la controparte potrebbe non essere in grado di provarne la falsità[18].

Come si è anticipato, la Suprema corte, nell'esaminare la tematica in oggetto, ha sostenuto la legittimità dell'acquisizione di una "fotografia dello schermo" ai sensi dell'art. 234 c.p.p.[19].

Alla luce delle considerazioni svolte *supra*, detta conclusione non appare censurabile.

La legge processuale, difatti, non impone alcun adempimento specifico per il compimento di tale attività, che si riduce, sostanzialmente, «nella realizzazione di una fotografia e che si caratterizza solamente per il suo oggetto, costituito, appunto, da uno schermo sul quale siano leggibili messaggi di testo, non essendovi alcuna differenza tra una tale fotografia e quella di qualsiasi altro oggetto, con la conseguente legittimità della sua acquisizione»[20].

Le perplessità, invece, sorgono con riguardo alle conseguenze processuali che la giurisprudenza trae dalla riconducibilità dello *screenshot* nel solco della prova documentale, ovverosia l'irrilevanza di ogni questione attinente alla genuinità del dato rispetto a eventuali istanze di parte dirette all'"esclusione probatoria" del materiale raccolto (*rectius*, inutilizzabilità)[21]. Facendo leva sul principio del libero convincimento, l'indirizzo pretorio ritiene perlopiù superflua ogni operazione (acquisizione e analisi del *device* o trascrizione della *chat*) diretta a saggiare la corrispondenza tra quanto raffigurato nello *screeshot* e la fonte digitale[22]. In mancanza di previsioni sanzionatorie esplicite, dunque, ogni censura relativa all'integrità del materiale probatorio è ritenuta soccombente rispetto a esigenze di non dispersione della prova.

Questo modo di argomentare, come si è anticipato, non sembra affatto convincente.

A fronte di un elevato rischio di contaminazione e di manipolazione delle prove estratte dai *social network*, la semplice produzione di uno *screenshot* non è idonea a garantire l'attendibilità del compendio probatorio *ivi* rappresentato. Detto obiettivo, per contro, può essere raggiunto solamente attraverso l'ostensione del supporto contenente l'originale del dato informatico, unica operazione che consente di verificarne la genuinità. È evidente, infatti, che la mera stampa di un messaggio, ad esempio, non può avere alcun valore

[18] D'altro canto, anche con riguardo al tema della prova scientifica, la Corte di cassazione ha affermato che «l'onere della prova sulla corretta acquisizione dei dati e sul fondamento della teoria posta a base della ricostruzione grava sulla parte che introduce il dato scientifico» (così, da ultimo, Cass., Sez. Un., 28 gennaio 2019, n. 14426).

[19] Cass. pen., Sez. V, 5 febbraio 2021, n. 12062.

[20] Cass. pen., Sez. III, 6 novembre 2019, n. 8332. Conformi, in seguito, Cass. pen., Sez. V, 26 aprile 2022, n. 24600; Cass. pen., Sez. V, 10 marzo 2021, n. 17552.

[21] Cass. pen., Sez. V, 6 ottobre 2021, n. 2658, la quale ha ritenuto legittima la scelta del giudice di prime cure di rigettare la richiesta della difesa volta a ottenere l'analisi del supporto telematico contenente le conversazioni *Whatsapp* introdotte dall'accusa.

[22] Cass. pen., Sez. II, 1° luglio 2022, n. 39529.

probatorio se non a seguito di una perizia che ne dimostri la provenienza[23]. Del resto, lo si è visto, pure la giurisprudenza spagnola e quella americana reputano che l'utilizzabilità del fermoimmagine debba essere condizionata all'acquisizione e all'analisi della strumentazione informatica.

Le Corti italiane, invero, vanno assumendo, a quest'ultimo proposito, una posizione assai peculiare.

Seppur timidamente, in alcune pronunce del giudice di legittimità è dato leggere che l'utilizzabilità dello *screenshot* deve ritenersi condizionata all'acquisizione del «supporto telematico o figurativo contenente la relativa registrazione, al fine di verificare l'affidabilità, la provenienza e l'attendibilità del contenuto di dette conversazioni»[24]. Ciò nondimeno, la portata di questa apprezzabile esegesi garantista è stata drasticamente circoscritta, in successivi arresti, alla luce del fatto che detta *regula iuris* non potrebbe essere invocata «in astratto»[25], senza cioè verificarne in concreto la pregnanza e la decisività. Il richiamo, operato dalla Corte nella summenzionata pronuncia, alla necessità di un controllo sull'affidabilità della prova, in altre parole, non riguarderebbe qualunque *screenshot*, bensì solo quelli rispetto ai quali gli elementi del caso di specie inducono il giudice, in base a una valutazione discrezionale e *case by case*, a ritenere indispensabile l'analisi forense del *device*.

Questo *modus pensandi* sembra risentire dell'impostazione nordamericana e, in specie, di quel *corroboration approach* che consente alle Corti d'oltreoceano di "sanare" i difetti di autenticità della prova *social* ricorrendo a elementi indizianti. Il mezzo di prova in grado di accertare la genuinità dello *screenhost*, in questa prospettiva, non è rappresentato dall'analisi del dispositivo (*rectius*, la perizia o la consulenza tecnica), bensì dall'impiego di inferenze logico-deduttive ricavate, perlopiù, dalle dichiarazioni di testimoni e persone offese. E allora, si percepisce, da parte della giurisprudenza, un atteggiamento di netta chiusura rispetto alla capacità "certificatrice" della *digital forensics*, posto che – seguendo questa linea di pensiero – sono le prove dichiarative a svolgere una sorta di surrogato di detta funzione.

Sembrano delinearsi, a questo proposito, due orientamenti diametralmente opposti.

Per un verso, come giustamente osservato in dottrina, il principio del libero convincimento non dovrebbe essere utilizzato per consentire, in ogni caso, l'ingresso processuale a un materiale probatorio, lo *screeshot*, la cui autenticità è ontologicamente incerta. Se ne è

[23] In senso contrario, v., esplicitamente, Cass. pen., Sez. VI, 6 febbraio 2020, n. 12975, par. 2.3: «è pacifico che la copia estratta da un documento informatico ha la medesima valenza probatoria del dato originariamente acquisito, salvo che se ne deduca e dimostri la manipolazione».

[24] Cass. pen., Sez. V, 25 ottobre 2017, n. 49016, par. 2; Cass. pen., Sez. II, 6 ottobre 2016, n. 50986. Pur non spingendosi fino a ritenere necessario l'esame del *device*, pure la Corte di Assise di Roma, 17 febbraio 2023, n. 2, in *Giurisprudenza penale* web, 28 febbraio 2023, p. 21, sottolinea come «il video scaricato dal canale *YouTube*, trattandosi di piattaforma *Internet* attraverso la quale vengono pubblicati nel *web* contenuti multimediali, deve ritenersi che lo stesso sia acquisibile quale prova documentale ai sensi dell'art. 234 c.p.p., salvo valutarne l'attendibilità e l'assenza di manipolazione».

[25] Cass. pen., Sez. V, 6 ottobre 2021, n. 2658, cit. Conforme, da ultimo, Cass. pen., Sez. VI, 28 giugno 2023, n. 38678, ove si legge che «per la concreta utilizzabilità della trascrizione delle conversazioni via *Whatsapp*, la necessità di acquisire il supporto telematico o figurativo contenente la relativa registrazione deve essere valutata in concreto».

ricavata – richiamando l'opinione espressa anni or sono da autorevole dottrina[26] – l'inutilizzabilità processuale per *unreliability* della prova in assenza dell'acquisizione materiale del supporto che la incorpora[27].

Per altro verso, l'atteggiamento pretorio che, valorizzando ragioni di stretta economia processuale, rinnega un approccio generalizzato al tema *de quo*, si mostra più incline a tutelare ragioni di efficienza e di stretta economia processuale. Un punto di vista, va detto, che non appare del tutto irragionevole, perlomeno laddove si ponga mente al rischio di contribuire, mediante il ricorso sistematico ad analisi forensi, alla creazione di una sorta di "statuto fideistico della perizia informatica"[28] che, in un'epoca nella quale il "soluzionismo tecnologico" pare ormai aver preso il sopravvento, mostra, però, tutti i suoi limiti[29].

I problemi, tuttavia, non si arrestano qui.

La questione più delicata attiene, infatti, alla natura spiccatamente e, verrebbe da dire, ontologicamente "transitoria" delle informazioni presenti nelle "reti virtuali".

A tal proposito, è possibile parlare di una "transitorietà estrinseca", cioè dipendente da fattori esterni, tutte le volte in cui il dato originale non sia più disponibile in Rete, giacché rimosso dal *provider* o cancellato dal suo stesso autore, come nel caso di un contenuto "postato" su *Facebook*.

Nel cyberspazio, però, vi è anche una "transitorietà intrinseca", connessa alle caratteristiche tecniche del singolo *social network*: ne sono un chiaro esempio i contenuti pubblicati su *Snapchat*[30], le *stories* diffuse su *Instagram*[31] o i messaggi inviati su *Whatsapp* con l'opzione "visualizza una volta"[32]. Si tratta, in linea generale, di casi nei quali i contenuti (pubblici, ristretti o privati) restano a disposizione della *community* o del singolo destinatario per pochi istanti o, al massimo, per poche ore, decorse le quali il sistema procede alla loro automatica cancellazione.

---

[26] L. LUPÁRIA, *Il caso "Vierika": un'interessante pronuncia in materia di* virus *informatici e prova penale digitale*, in *Dir. Internet*, 2006, p. 195 ss., il quale, primo nel panorama nazionale, ha teorizzato l'inutilizzabilità di quel materiale di prova digitale raccolto in maniera tale da non assicurare un accertamento attendibile dei fatti di reato.

[27] Per questa opinione, v., ad es., G. FIORELLI, *Lo* screenshot *quale prova* documentale, cit., p. 509.

[28] In proposito, autorevole dottrina spagnola ha descritto tale fenomeno in termini di *«"sumisión" o "sometimiento" pericial*», ovverosia «*un exceso de dependencia de las autoridades de persecución penal - singularmente, de las autoridades judiciales- respecto de los informes periciales*» (F. GASCÓN INCHAUSTI, *Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial*, in AA.VV., *La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro*, Barcellona, 2019, p. 200).

[29] D'altro canto, il proliferare, negli ultimi anni, del numero dei casi di errori giudiziari conseguenti a perizie scientifiche rivelatesi *ex post* inaffidabili, imprecise o inadeguate, dovrebbe mettere in guardia da simili conclusioni.

[30] Trattasi di un *social network* che consente ai propri utenti di scambiarsi foto e video che vengono cancellati automaticamente decorse ventiquattro ore dalla visualizzazione ad opera del destinatario.

[31] Le *Instagram Stories* possono essere definite, con una buona dose di approssimazione, come contenuti multimediali temporanei (video, foto o testi) che restano visibili sul profilo dell'utente per un periodo di ventiquattro ore dalla pubblicazione, a seguito del quale sono automaticamente rimosse.

[32] Il riferimento è alla nuova funzionalità messa a disposizione da *Whatsapp* che consente di inviare messaggi, foto e video che non sono più visibili dopo essere stati aperti dal destinatario. Una volta visualizzato, infatti, il *file* multimediale non sarà più presente nella *chat* e non potrà essere visto nuovamente. Per garantire la *privacy* dei propri internauti, il SNP ha recentemente deciso di inibire la possibilità di realizzare *screenshot* con riguardo ai messaggi inviati in modalità "visualizza solo una volta" *https://faq.whatsapp.com/1077018839582332/?locale=it_IT*.

In entrambe le ipotesi, il dato originale non è più disponibile, inibendo la possibilità di esperire le operazioni dirette alla verifica della sua genuinità. Il tema, com'è intuibile, si fa particolarmente "caldo" specialmente qualora l'informazione costituisca essa stessa corpo del reato[33] o la prova audio-video delle violenze perpetrate a danno della vittima.

La dottrina più accorta, in realtà, si è già confrontata con questa problematica, giungendo a conclusioni che, pur apprezzabili, non appaiono del tutto soddisfacenti.

Alcuni autori, adottando una posizione di assoluto rigore, hanno negato "cittadinanza processuale" a tutti i fermo-immagine rappresentativi di dati digitali non più esistenti in *rerum natura*[34]. L'impossibilità oggettiva di testarne la genuinità – secondo questa corrente di pensiero – giustificherebbe l'operare di una vera e propria regola di esclusione, negando alla prova qualsiasi valenza epistemologica.

Un simile approccio, ancorché volto a tutelare l'affidabilità dell'accertamento, cioè la sua validità gnoseologica – rispetto alla quale la genuinità del dato informatico costituisce la *conditio sine qua non* – sembra non tenere conto a sufficienza del pregiudizio connesso alla rinuncia *tout court* di materiale che, nella prassi, si rivela spesso di fondamentale importanza[35].

Proprio l'esigenza di non disperdere materiale processualmente rilevante ha indotto alcuni commentatori a propendere per una sorta di "acquisizione vicaria" del materiale non più disponibile, riconoscendo in tal modo la piena utilizzabilità dello *screenshot*[36]. In dette circostanze – si sostiene – il «"difetto genetico" di autenticità»[37] che caratterizza lo "scatto fotografico digitale" dovrebbe essere compensato da un maggior rigore motivazionale richiesto al giudice sul versante del controllo in sede di ammissibilità e valutazione della prova.

Pure una conclusione siffatta appare, tuttavia, eccessivamente *tranchant*.

Si consideri, nuovamente, l'ipotesi di una storia pubblicata su *Instagram* o un messaggio inviato mediante l'applicativo *Snapchat*. Nel primo caso, il dato potrebbe essere recuperato direttamente mediante l'archivio presente nell'applicazione o a seguito di un esame forense del *device*. Quanto al secondo, alcune tra le più importanti compagnie americane di *digital forensics* hanno sviluppato *software* in grado di recuperare i cd. *delated Snaps* mediante un'"irruzione informatica" nel dispositivo[38].

Quid iuris, però, nel caso in cui pure dette operazioni si rivelino, in concreto, non praticabili?

Un'opzione potrebbe essere quella di istituire un meccanismo che consenta di rivolgersi al *social network provider* per ottenere l'originale del dato. Anche questa soluzione, però,

---

[33] Si pensi alla pubblicazione di un *post* diffamatorio, in seguito rimosso.

[34] Parrebbe adottare tale impostazione G. FIORELLI, *Lo* screenshot *quale prova* documentale, cit., p. 509 s.

[35] Parimenti critico, in tal senso, pure M. PITTIRUTI, Digital evidence *e procedimento penale*, Torino, 2017, p. 26.

[36] R. DEL COCO, *L'utilizzo probatorio dei dati* whatsapp, cit., p. 539, che si riferisce, per l'appunto, allo *screeshot* come a una «fattispecie documentale vicaria».

[37] Ancora, R. DEL COCO, *L'utilizzo probatorio dei dati* whatsapp, cit., p. 539 s.

[38] Ne dà conto, più nel dettaglio, M. BUNGERT, *Do it For the Snap: Different Methods of Authenticating Snapchat Evidence for Criminal Prosecutions*, in *University of Illinois Journal of Law, Technology & Policy*, 2021, p. 138.

potrebbe non essere del tutto appagante, specialmente con riguardo a tutte quelle informazioni trasmesse (e, in seguito, screenshottate) attraverso linee *Internet* crittografate. In questi casi, lo si è detto, neppure il *provider* è in grado di accedere al contenuto, rendendo *de facto* impossibile la realizzazione di operazioni di autenticazione *ex post* e, prima ancora, il reperimento del dato informatico originale.

Per tentare di risolvere il problema, potrebbe a primo acchito sostenersi l'applicabilità dell'art. 234, comma 2, c.p.p. La disposizione, come noto, consente al giudice di acquisire la copia di un documento (e, dunque, anche di quello nativo digitale) qualora l'originale non sia più disponibile, proprio come nel caso di uno *schreenshot* (documento cartaceo) rappresentativo di un *quid* informatico che non è possibile recuperare in alcun modo. La fallacia di tale argomentazione emerge *icto oculi*: la riproduzione del documento informatico incorporata nella "fotografia dello schermo" non è in grado di garantire il crisma dell'autenticità.

Le numerose difficoltà riscontrate e l'inadeguatezza delle differenti soluzioni prospettate, pertanto, inducono a riflettere sull'opportunità di saggiare nuove prospettive per garantire i canoni della genuinità e non alterazione del dato digitale "*on the social*".

A fronte della transitorietà ontologica delle prove presenti nelle *web communities*, sembra che l'unico strumento in grado di garantire tale obiettivo sia quello di intervenire a monte, nel momento stesso in cui il dato digitale viene a esistenza. Potrebbero essere recuperate e spese, pure in questa sede, le considerazioni già offerte *supra* con riguardo alla certificazione preventiva delle informazioni *open access*. Si potrebbe immaginare, cioè, di introdurre una disciplina legislativa che consenta – tanto alla polizia giudiziaria (introducendo, in tal caso, un vero e proprio obbligo), quanto ai privati cittadini – l'impiego di strumenti informatici di certificazione preventiva della genuinità delle informazioni digitali.

Questa soluzione consentirebbe di superare le problematiche legate all'utilizzo processuale dello *screenshot*. Difatti, pure quando il contenuto originale non risulti più presente nei *server* del *provider* o non sia comunque apprensibile, l'impiego anticipato dei *software* di analisi consentirebbe di cristallizzare la prova, escludendo così ogni dubbio su una eventuale manipolazione precedente o successiva rispetto all'atto di certificazione. Per di più, l'impiego di sofisticati algoritmi di analisi permetterebbe di ridurre quelle asimmetrie tra accusa e difesa, posto che dette attrezzature informatiche risultano accessibili al pubblico con un dispendio di risorse assai più ridotto rispetto a quello necessario per l'esecuzione, *ex post* e con esiti a tratti persino più incerti, di una consulenza tecnica o di una perizia.

4. L'accertamento della paternità dei contenuti presenti nelle piattaforme

Per dimostrare l'autenticità *lato sensu* intesa di uno *screenshot*, il giudice è chiamato a operare una duplice valutazione[39]. In primo luogo, occorre verificare se quanto *ivi* cristallizzato rifletta effettivamente il contenuto di un'immagine o di un testo presente in un *social network*. Accertata l'esistenza *in rerum natura* della raffigurazione contenuta nello *screenshot*, è necessario, in seguito, valutarne la genuinità. Questi profili, come si è detto,

[39] W. ANGUS-ANDERSON, *Authenticity and Admissibility of Social Media Website Printouts*, in *Duke Law & Technology Review*, 2015, p. 44 s.

potrebbero essere "certificati" grazie all'impiego di algoritmi in grado di cristallizzare il dato digitale nel momento in cui un soggetto ne viene a conoscenza.

Ciò, tuttavia, non è sufficiente per ritenere superato il *test* di autenticità.

La prova di non alterazione, infatti, impedisce di riferire soggettivamente quello specifico contenuto a una determinata persona. L'anonimato che caratterizza, in generale, le attività compiute in Rete non consente di svolgere una inferenza diretta tra il titolare dell'*account*, l'effettivo utilizzatore e l'autore del singolo contenuto.

A questo riguardo, assume certamente rilievo la tematica relativa al documento anonimo, la cui disciplina è attualmente incardinata nell'art. 240 c.p.p.

In relazione allo *screenshot* – ma, invero, pure con riguardo a ogni altra tipologia di documento – il concetto di anonimato e, di riflesso, quello di paternità, può essere astrattamente inteso in una duplice prospettiva, occorrendo distinguere il soggetto che ha "creato" il fermo immagine dall'autore di quando *ivi* rappresentato[40].

Nel caso che ci occupa, a ben riflettere, il *punctum dolens* non concerne tanto l'individuazione dell'artefice materiale dello *screenshot* (e della successiva stampa della quale si invoca l'ammissione). L'art. 239 c.p.p., infatti, consente alle parti e al giudice, al fine di verificare la provenienza di un documento, di sottoporlo all'attenzione di terzi (ad esempio, un testimone). In concreto, dunque, è sufficientemente agevole – e la prassi giudiziaria ne dà prova – identificare chi abbia concretamente eseguito l'istantanea, trattandosi perlopiù di un "pezzo di carta" proveniente dall'imputato, dalla vittima o dalla polizia giudiziaria (che lo ha acquisito, il più delle volte, in sede di verbalizzazione di un atto di querela o nel corso delle sommarie informazioni testimoniali).

Il problema, invece, riguarda l'identificazione dell'autore morale o ideologico, cioè colui al quale è materialmente attribuibile il contenuto (dichiarativo, visivo, etc.) estratto dalla *chat Whatsapp* o pubblicato su un altro *social network*. Anche qualora si dimostrasse la corrispondenza tra il titolare effettivo di quel determinato *account* e il soggetto al quale esso è asseritamente attribuito, ciò non sarebbe comunque sufficiente, lo si è visto, per indurre la riferibilità del contenuto a detto individuo.

Il caso con il quale occorre confrontarsi attiene, dunque, al trattamento processuale dello *screenshot* di autore noto che contiene materiale proveniente da soggetto ignoto.

Seguendo l'insegnamento – pur non unanimemente condiviso – di autorevole dottrina, ciò che rileva, ai fini dell'utilizzabilità di un documento, è l'accertamento della paternità di quanto *ivi* contenuto (essendo irrilevante, per contro, l'identificazione dell'autore materiale)[41]. Laddove, quindi, non si riesca a dimostrare la paternità ideologica, lo *screenshot* dovrebbe essere ritenuto inutilizzabile *ex* art. 240, comma 1, c.p.p.

A monte, com'è intuibile, si staglia il problema dell'*iter* procedimentale da seguire per accertare la paternità del contenuto ricavato dai *social network*. Che si tratti di uno *screenshot* rappresentativo di un'immagine o di una *chat* ovvero di un qualunque altro dato

[40] Si prenda il caso in cui un "navigante del *web*" che esegua uno *screenshot* di un *post* pubblicato su *Facebook* da un terzo cibernauta.

[41] F. CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, p. 323. *Contra*, F. ZACCHÈ, *La prova documentale*, cit., p. 69.

presente nelle piattaforme, per poter utilizzare quel materiale probatorio occorre individuare con certezza il suo autore.

Il tema può essere approcciato muovendo dall'esame della giurisprudenza formatasi, in prevalenza, in materia di diffamazione a mezzo *Facebook*. Vi sono già taluni casi, infatti, nei quali le Corti di merito e i giudici di legittimità sono stati chiamati a individuare criteri logico-argomentativi per giustificare la riconducibilità di una propalazione illecita a un determinato soggetto.

In proposito, triplice sembra essere l'alternativa astrattamente prospettabile.

Si potrebbe ritenere, in ogni caso, necessaria e sufficiente, l'acquisizione dell'indirizzo IP associato al profilo *social* di interesse, dal momento che l'*Internet Protocol*, come ormai risaputo, è in grado di identificare univocamente uno specifico *device* (*rectius*, un nodo) all'interno della Rete.

Una seconda possibilità è quella di considerare l'apprensione dell'indirizzo IP necessaria, ma non sufficiente, per provare la riferibilità del contenuto a una determinata persona, occorrendo, altresì, la presenza di ulteriori indizi univocamente rappresentativi della paternità dell'*account* (e, di riflesso, del *post* o del messaggio).

Infine, si potrebbe reputare superfluo l'ottenimento dell'IP in presenza di ulteriori elementi di prova convergenti verso una riferibilità inequivoca del contenuto in capo al supposto autore.

L'approccio da ultimo ipotizzato, benché affatto condivisibile, è stato accolto dalla giurisprudenza maggioritaria.

A tal riguardo, infatti, la Suprema corte suole affermare che la riferibilità all'imputato di un *post* a contenuto diffamatorio può ritenersi provata, pur in mancanza di accertamenti circa la provenienza da uno specifico indirizzo IP, su base indiziaria, ossia alla luce di circostanze ed elementi fattuali convergenti, plurali e precisi[42]. Tra questi, si è attribuito specifico rilievo all'accertamento della provenienza del *post* o del messaggio dalla bacheca virtuale riconducibile all'imputato, all'assenza di una denuncia per furto di identità digitale[43] e al contenuto della pubblicazione (specialmente qualora essa riporti con dovizia di dettagli episodi dei quali solo l'imputato poteva essere a conoscenza). Si tratta – ad avviso del Supremo consesso – di parametri che, se correttamente valorizzati attraverso il ricorso a criteri logici e massime di esperienza condivise[44], «finiscono per svolgere un'insuperabile portata individualizzante»[45], in grado di provare, oltre ogni ragionevole dubbio, la riferibilità soggettiva del materiale probatorio di cui si discute.

Un'impostazione di questo tipo, lo si è accennato, non può essere acriticamente condivisa.

---

[42] Cfr. Cass. pen., Sez. V, 7 settembre 2023, n. 39692, par. 2, ove si esplicita quanto segue: «questa Corte non ha mai asserito che l'acquisizione di tali dati e di quelli di connessione (c.d. *file* di *log*) sia adempimento imprescindibile al fine di attribuire la paternità di uno scritto pubblicato sui *social network*». Conforme, Cass. pen., Sez. V, 23 settembre 2022, n. 39805.

[43] Cass. pen., Sez. V, 13 luglio 2018, n. 45339; Cass. pen., Sez. V, 13 luglio 2015, n. 8328; Cass. pen., Sez. V, 29 ottobre 2015, n. 8275.

[44] Cass. pen., Sez. V, 21 ottobre 2021, n. 4239.

[45] Cass. pen., Sez. V, 23 settembre 2022, n. 39805, cit.

Come messo in luce in un'isolata (ma alquanto significativa) pronuncia di legittimità, ancorché in presenza di indizi apparentemente stringenti e convergenti in ordine all'identificazione di un soggetto quale autore del reato, «il presupposto imprescindibile per giungere ad una corretta motivazione sottesa ad una pronuncia di condanna» è provare «con certezza la riconducibilità del *post* diffamatorio agli imputati, attività possibile, però, soltanto attraverso il reperimento dell'indirizzo IP»[46]. La corretta individuazione del codice numerico assegnato in via esclusiva a ogni dispositivo elettronico che si colleghi alla Rete, infatti, è l'unico elemento in grado di attestare l'effettiva titolarità dell'*account* attraverso l'intestazione della linea telefonica allo stesso associata.

Quanto detto, è opportuno precisarlo, non può condurre a sostenere che la mera acquisizione dell'IP sia di per sé sufficiente a provare la genuinità *lato sensu* intesa del contenuto estrapolato dal *social network*. Benché talvolta si sia tentato di sostenere, pure in sede pretoria[47], che l'*Internet Protocol Address* consente di risalire, senza possibilità di equivoci, a un solo e unico dispositivo, i tecnici informatici insegnano, invece, che gli aspetti infrastrutturali delle reti portano a dubitare dell'affermazione secondo cui un indiritto IP «identifica "univocamente" un apparato in *Internet* e quindi tendenzialmente un utente»[48].

Alla luce di tali considerazioni, dunque, sembra preferibile ricorrere a un approccio "logico-tecnologico": in presenza di indizi apparentemente stringenti e convergenti in ordine all'identificazione di un soggetto quale autore del contenuto *social*, il pubblico ministero è chiamato, in ogni caso, a reperire l'indirizzo IP mediante il quale ritiene sia stata operata la connessione.

[46] Cass. pen., Sez. V, 22 novembre 2017, n. 5352. Nello stesso senso, tra le pronunce di merito, Tribunale di Rovigo 12 giugno 2019, n. 331.

[47] Cass. pen., Sez. V, 18 settembre 2015, n. 38099.

[48] Testualmente, G. COSTABILE, *Rete* Internet *e "dintorni": aspetti tecnici di base*, in AA.VV., Cyber forensics *e indagini penali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, p. 34, al quale si rinvia per una più dettagliata disamina delle cause *stricto sensu* informatiche legate a detto fenomeno (p. 34-42).

Brevi osservazioni conclusive

Nel corso del presente studio, si è tentato di ricostruire i molteplici e intricati legami esistenti tra il "fenomeno *social*" e il sistema di giustizia penale. Tra questi, il settore che mostra maggiori criticità, specie sul versante della tutela dei diritti fondamentali, è rappresentato dall'impiego di informazioni estrapolate dalle piattaforme digitali per finalità investigative e probatorie.

Giunti all'epilogo dell'elaborato, dunque, pare opportuno soffermarsi – senza alcuna velleità riepilogativa – proprio su questo particolare aspetto della trattazione.

Innanzitutto, se si volesse rintracciare una sorta di *fil rouge* del percorso ricostruttivo qui svolto, esso potrebbe essere certamente individuato nella carenza di legittimazione normativa che riguarda la maggior parte dei mezzi di ricerca della prova esaminati. Lo si è osservato: tanto il *social network patrolling*, quanto la *false friends technique* (nonché, per certi aspetti, anche le operazioni di indagine più tradizionali) scontano un marcato *deficit* di legalità processuale. In assenza di previsioni chiare e precise, principi-cardine del sistema giuridico italiano, quali il principio di uguaglianza e quello di separazione dei poteri, rischiano di essere sacrificati al cospetto di atti investigativi compiuti arbitrariamente dall'autorità pubblica.

Questa considerazione è destinata ad assumere un certo rilievo qualora si ponga mente al fatto che tali mezzi di ricerca della prova, finalizzati all'apprensione di *bit* digitali, hanno un impatto significativo sulle libertà fondamentali degli individui e, in specie, sul diritto alla riservatezza e alla tutela della vita privata (art. 8 CEDU). Si è osservato, infatti, come la *privacy*, pure nella sua dimensione "interpersonale", costituisca una garanzia la cui effettività deve essere assicurata indipendentemente dalla natura e dall'accessibilità del dato informatico. E, in effetti, nel caso in cui un soggetto abbia deciso – volontariamente e consapevolmente – di rendere "pubblici" o "ristretti" certi contenuti, l'autorità perquirente non può ritenersi, per ciò solo e *de iure condito*, legittimata alla loro raccolta massiva e alla successiva conservazione.

Come si è cercato di dimostrare, però, tali problematiche non possono essere affrontate negando *tout court* "diritto di cittadinanza" a queste nuove metodologie di indagine. Allo stato attuale, infatti, non sembra possibile prescindere da un loro impiego per finalità di prevenzione e di repressione criminale, ma ciò, per l'appunto, solo a condizione che simili attività risultino minuziosamente disciplinate. Del resto, già agli inizi degli anni '80 del secolo scorso, illustre dottrina ebbe modo di osservare come in presenza di evoluzioni tecnologiche, pur repentine e ineluttabili, non si debba comunque «rinunciare a norme ancorate al principio di legalità»; norme che, se necessario, «devono essere progressivamente adattate, dal punto di vista sostanziale e processuale, ai mutevoli bisogni [della collettività]»[1].

[1] P. NUVOLONE, *Funzionamento e prospettive della giustizia penale in un mondo in evoluzione*, in *Ind. pen.*, 1983, p. 240.

D'altra parte, che il nucleo essenziale della questione – e, quindi, per molti aspetti, anche la sua soluzione – risieda nel rispetto del principio di legalità processuale o, più precisamente, nella necessità di una copertura normativa delle attività investigative qui esaminate, è confermato pure da recenti provvedimenti adottati – ancorché in un diverso contesto – dall'*European Data Protection Supervisor*[2]. Nel censurare le operazioni di *social network patrolling* realizzate dall'Ufficio di sostegno per l'asilo[3], l'Autorità per la protezione dei dati personali ha stabilito che le agenzie comunitarie debbano non solo avere una specifica base giuridica per effettuare una qualunque forma di monitoraggio delle piattaforme (indipendentemente dalla finalità perseguita, nel caso di specie, senz'altro lodevole), ma anche predisporre adeguate e robuste garanzie di ordine procedimentale.

Proprio l'interesse manifestato in questa materia dagli organismi di controllo e vigilanza, nonché, dalle Corti europee (del quale si è dato conto nel corso della trattazione) dovrebbe indurre, in una prospettiva *de iure condendo*, a individuare precisamente nell'ordinamento sovranazionale il punto di riferimento per future iniziative legislative. Del resto, le Istituzioni comunitarie sembrano aver preso consapevolezza, almeno in parte, dell'elevata intrusività, sul versante delle libertà fondamentali, di attività volte alla raccolta massiva di informazioni di carattere personale (a prescindere dalla loro accessibilità). L'adozione della più volte richiamata Direttiva 2016/680/UE muove, difatti, dall'idea per cui gli strumenti tecnologici contemporanei consentono alle autorità statali, come mai in precedenza, di trattare una quantità enorme di dati per finalità preventive e repressive dei fenomeni criminosi.

Sotto questo profilo, e rifacendosi alle considerazioni svolte *supra* in merito all'approccio normativo da adottare con riguardo ai fenomeni *online*, è auspicabile un intervento europeo volto a stabilire i principi generali e a disegnare la cornice di garanzie entro la quale potranno muoversi i legislatori nazionali. E ciò, specie nella prospettiva italiana, ove la già ricordata vicenda della Direttiva 2016/680/UE (rispetto alla quale ci si è limitati a recepirne pedissequamente il contenuto) rende ancor più urgente l'introduzione di una disciplina organica della materia.

A tal proposito, sono destinati ad assumere un certo rilievo – come si è cercato di sottolineare – il ruolo e le funzioni che si vogliano attribuire al giudice per le indagini preliminari, nella veste di garante della "fase istruttoria".

È evidente, infatti, che, in un contesto nel quale le tecniche investigative appaiono sempre più indirizzate verso una raccolta massiva di dati, con un conseguente spostamento dell'asse del processo dal dibattimento alla "fase previa", il «principio dell'irrilevanza probatoria delle attività compiute prima del giudizio»[4] rischi definitivamente di rimanere mero *flatus vocis*.

---

[2] EUROPEAN DATA PROTECTION SUPERVISOR, *Annual Report*, 2019, p. 30.

[3] Oggi denominato *European Union Agency for Asylum*. L'EASO utilizzava *software* di *network-patrolling* per rilevare informazioni pubblicamente disponibili nelle piattaforme di comunicazione (dati identificativi, età, sesso, nazionalità, commenti sul traffico di esseri umani, immagini, video, etc.), al fine di ottenere una panoramica generale sullo *status* migratorio a livello europeo, contribuendo così a implementare un'applicazione efficace e uniforme, negli Stati membri, della legislazione in materia di asilo (*https://euaa.europa.eu/sites/default/files/Record_on_Social_Media_Monitoring_Reports_2020_24.pdf*).

[4] E. MARZADURI, *Inviolabilità della difesa e trasformazioni del processo*, in D. Negri – L. Zilletti (a cura di), *Nei limiti della Costituzione. Il Codice Repubblicano e il processo penale contemporaneo*, Milano, 2019, p. 122.

Sembra tornare in auge, così, l'interrogativo posto dall'illustre Autore all'indomani dell'entrata in vigore del Codice Vassalli: «ma è poi vero che quelle acquisizioni conoscitive [apprese nelle indagini preliminari] non costituiscono in alcun senso delle prove?»[5].

A fronte di strumenti investigativi che consentono all'autorità pubblica di ottenere, già nella fase dell'"inchiesta", elementi di prova precostituiti (o, meglio, *ab origine* irripetibili), sarebbe illusorio, pertanto, ritenere che l'efficacia delle investigazioni si esaurisca all'interno del momento pre-processuale. Per tale ragione, dunque, sarebbe opportuno introdurre, dal punto di vista normativo, un vaglio di tipo giurisdizionale operato da un organo *super partes*. L'emergere di nuove tecniche *lato sensu* captative, del resto, non può che condurre verso un rafforzamento di quella "giurisdizione di garanzia" che, unitamente alla "giurisdizione sulle libertà", contribuisce a qualificare il GIP come figura «polifunzionale»[6], il cui compito è appunto quello di assicurare un'adeguata tutela dei diritti dell'indagato[7].

È in questa direzione, d'altro canto, che si è già mosso il legislatore nazionale sul terreno della *data retention*. Il percorso di riforma inaugurato con il d.lgs. 30 settembre 2021, n. 132 – con il quale il Parlamento ha attribuito al GIP il potere di autorizzare l'acquisizione dei tabulati telefonici – è auspicabile possa proseguire pure con riguardo alle nuove metodologie di indagine nei *social network* esaminate nella presente trattazione (pur con le precisazioni delle quali si è detto) –, parimenti invasive della sfera di libertà individuale.

Sempre nella prospettiva di una sistematizzazione legislativa della materia, occorre, poi, considerare il ruolo ricoperto dai gestori delle piattaforme di *sharing* nel contesto delle indagini penali.

Il dibattito sul tema si è fatto, specie negli ultimi anni, piuttosto vivace. Al netto delle diverse posizioni emerse, un dato appare indubbiamente incontestabile: i *Social network provider* detengono, di fatto, il controllo esclusivo sui contenuti processualmente rilevanti presenti in Rete. Di qui, come si è cercato di dimostrare, la necessità di un loro coinvolgimento nel corso della fase investigativa (sul versante nazionale, transfrontaliero e anche con riguardo alle indagini presso la *International Criminal Court*), con la finalità di garantire l'apprensione di informazioni *online*, comprese quelle rimosse dalle *web communities* per garantire l'esistenza di uno "spazio virtuale" sicuro e accessibile. Il percorso da seguire, occorre precisarlo, non è certo quello di predisporre "deleghe investigative in bianco" a favore di questi soggetti privati, bensì quello di coinvolgerli, nell'ottica di una collaborazione (esternalizzazione) virtuosa, nell'esercizio della funzione perquirente.

Da ultimo, merita di essere sottolineato un dato emerso dall'analisi condotta con riguardo alla fase strettamente processuale[8].

Ci si riferisce al generale senso di smarrimento mostrato dalle Corti di merito e di legittimità (italiane e non solo) a fronte di un impiego sempre più massivo, a fini probatori,

[5] M. NOBILI, *Scenari e trasformazioni del processo penale*, Padova, 1998, p. 35.
[6] V. GREVI, *Funzioni di garanzia e funzioni di controllo del giudice nel corso delle indagini preliminari*, in AA.VV., *Il nuovo processo penale. Dalle indagini preliminari al dibattimento*, Milano, 1989, p. 15.
[7] F. RUGGIERI, *La giurisdizione di garanzia nelle indagini preliminari*, Milano, 1996, p. 16.
[8] Parte III.

di informazioni estrapolate dalle *web communities*. Ciò che affiora dallo studio del dibattito giurisprudenziale e dottrinale sviluppatosi *ultra fines* è il delinearsi di due approcci diametralmente opposti. Per un verso, vi è chi ritiene necessario un *upgrade* normativo per far fronte alle problematiche sul versante dell'autenticità della *social network evidence* connesse alla natura instabile degli *user generated content*; e, per altro verso, chi non intravede alcuna valida ragione per giustificare *standard* o parametri di ammissione e valutazione più stringenti rispetto a quelli comunemente previsti per la "prova analogica".

Nel panorama nazionale, per contro, gli (ancora, pochi) autori che si sono confrontati con dette tematiche sembrano essersi focalizzati prevalentemente sulla ricerca di letture interpretative in grado di contenere il rigore esegetico adottato dalla Suprema corte. Difatti, la prova documentale, nella prospettiva della Cassazione, rappresenta una sorta di "valvola di accesso" per l'ingresso dibattimentale della *social network evidence*.

Se, però, come si è cercato di mettere in rilievo, il documento (*rectius*, la disciplina dettata all'art. 234 c.p.p.) non è in grado di offrire garanzie sufficienti circa l'attendibilità del materiale *ivi* incorporato, appare necessario volgere lo sguardo altrove, alla ricerca di soluzioni capaci di conciliare la volatilità delle informazioni presenti nelle "reti virtuali" con l'intrinseca esigenza di stabilità e certezza propria del rito penale.

Nei *social network* tutto è fugace e passeggero, e quanto vi è rappresentato può svanire in un istante; il processo penale, da par sua, presuppone, invece, un elevato grado di attendibilità e affidabilità del compendio conoscitivo fonte dell'accertamento. In questa prospettiva, come si è cercato di evidenziare, il ricorso a forme di "certificazione preventiva" della genuinità degli elementi reperiti *online* potrebbe contribuire a rendere più stabili e, quindi, anche maggiormente affidabili, dal punto di vista probatorio, i contenuti digitali.

A conclusione dell'elaborato non può che svolgersi un'ulteriore e, forse, ovvia, constatazione.

Al cospetto di un'imponente digitalizzazione degli strumenti investigativi e della fase probatoria, il processualpenalista non può fare altro che osservare l'evolversi del fenomeno tecnologico[9], prospettando, di volta in volta, soluzioni capaci di contemperare le esigenze di accertamento del fatto con i diritti e le garanzie dell'accusato. *Nihil sub sole novum*, vien da pensare: «naturalmente, l'utilizzazione della macchina porta con sé rischi e pericoli, suscitando, al tempo stesso, problemi di nuovo tipo e di non agevole soluzione. Nulla di strano che sia così: è lo scotto normale di ogni innovazione. Una sola cosa importa: prevenire i rischi, cautelarsi di fronte ai pericoli, studiare i problemi»[10].

[9] O, meglio, di quel «triplice insieme», rappresentato dal connubio fra scienza, tecnologia e intelligenza artificiale, che, come osservato da autorevole dottrina, pone ormai quotidianamente nuove sfide allo studioso del rito penale (in questi termini, M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., G*iurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 61).

[10] G. CONSO, *Macchine elettroniche e nuove prospettive giuridiche*, in *Riv. it. dir. proc. pen.*, 1971, p. 669.

BIBLIOGRAFIA

AGUSTINOY GUILAYN A. – MONCLÚS RUIZ J., *Aspectos Legales de las Redes Sociales*, Madrid, 2021

ALESSI G., *Il processo penale. Profilo storico*, Roma-Bari, 2007

ALI C.B., *International Crimes in the Digital Age: Challenges and Opportunities Shaped by Social Media*, in *Groningen Journal of International Law*, 2021, p. 43 ss.

ALLEGREZZA S., *Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione europea*, in D. Negri (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 59 ss.

ALLEGRI M.R., Ubi Social, Ibi Ius. *Fondamenti costituzionali dei* social network *e profili giuridici della responsabilità dei* provider, Milano, 2018

AMARELLI G., *Dalla legolatria alla post-legalità: eclissi o rinnovamento di un principio?*, in *Riv. it. dir. proc. pen.*, 2018, p. 1406 ss.

AMATO G., sub *Art. 14 Cost.*, in G. Branca (a cura di), *Commentario alla Costituzione*, Bologna-Roma, 1977, p. 57 ss.

AMATO G., *Individuo e autorità nella disciplina della libertà personale*, Milano, 1967

AMODIO E., *L'esame dell'imputato e la sua mutazione genetica*, in *Discrimen*, 5 luglio 2023

AMODIO E., *Estetica della giustizia penale. Prassi,* media *e* fiction, Milano, 2016

AMODIO E., *Garantismo e difesa sociale nel nuovo rito accusatorio*, in G. Riccio (a cura di), *Dalle indagini preliminari alla sentenza di primo grado*, Napoli, 1979, p. 239 ss.

AMODIO E., *Diritto al silenzio o dovere di collaborazione? A proposito dell'interrogatorio dell'imputato in un libro recente, in Riv. dir. proc.*, 1973, p. 412 ss.

AMORTH A., *La Costituzione italiana. Commento sistematico*, Milano, 1948

ANDOLINA E., *L'ammissibilità degli strumenti di captazione dei dati personali tra* standard *di tutela della* privacy *e onde eversive*, in *Arch. pen.*, 2015, p. 916 ss.

ANDREWS L., *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*, Londra, 2013

ANGLANO C., Cloud forensics *e prova digitale: problematiche e soluzioni*, in *Informatica e diritto*, 2015, p. 281 ss.

ANGUS-ANDERSON W., *Authenticity and Admissibility of Social Media Website Printouts*, in *Duke Law & Technology Review*, 2015, p. 33 ss.

APRATI R., *La notizia di reato nella dinamica del procedimento penale*, Napoli, 2010

APRUZZESE A., *La recente normativa in tema di contrasto del terrorismo e del proselitismo tramite* web*. Nuovi modelli di normative di prevenzione e nuovi schemi di indagini proattive*, in AA.VV., *La giustizia penale preventiva. Ricordando Giovanni Conso*, Milano, 2016, p. 229 ss.

ARIEL GENDLER M. – RULLANSKY I. – ABIUSO F.L., *Vigital y castigar en pandemia. Desafios teòrico-metodològicos en torno a la (in)definicòn del "ciberpatrullaje"*, in *Revista de la carrera de sociologìa*, 2022, p. 494 ss.

ARISTOTELE, *Politica*, Bari, 2007

ARMENTA DEU T., *Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambio*, Madrid, 2021

ARMENTA DEU T., *Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre*, in *Revista de Internet, Derecho y Política*, 2018, 27, p. 67 ss.

ARONSON D., *The Utility of User-Generated Content in Human Rights Investigations*, in M.K. Land – J.D. Aronson (a cura di), *New Technologies for Human Rights Law and Practice*, Cambridge, 2018, p. 129 ss.

ARONSON D., *Mobile Phones, Social Media and Big Data in Human Rights Fact-Finding: Possibilities, Challenges, and Limitations*, in P. Alston – S. Knuckey (a cura di), *The Transformation of Human Rights Fact-Finding*, New York, 2016, p. 441 ss.

ARRABAL PLATERO P., *La prueba tecnològica: aportaciòn, pràctica y valoraciòn*, Valencia, 2020

ASHOURI A. – BOWERS C. – WARDEN C., *An Overview of the Use of Digital Evidence in International Criminal Courts*, in *Digital Evidence and Electronic Signature Law Review*, 2014, p. 115 ss.

ATERNO S. – CAJANI F., *L'acquisizione dei dati di traffico*, in AA.VV., Cyber Forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, p. 270 ss.

ATERNO S., Cloud Forensics: *aspetti giuridici e tecnici*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 1949 ss.

ATERNO S., *L'acquisizione dei dati personali tra misure antiterrorismo e intromissioni nella* privacy, in *Arch. pen*., 2016, p. 165 ss.

BACCARI G.M. – CONTI C., *La corsa tecnologica tra Costituzione, codice di rito e norme sulla* privacy*: uno sguardo d'insieme*, in *Dir. pen. proc.*, 2021, p. 711 ss.

BACHMAIER WINTER L., *Sorveglianza, indagati e diritti fondamentali: sfide nella lotta al terrorismo in UE*, in V. Militello – A. Spena (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Torino, 2018, p. 209 ss.

BACHMAIER WINTER L., *Registro remoto de equipos informàticos y principio de proporcionalidad en la Ley Orgànica 13/2015*, in *Boletìn del Ministerio de Justicia*, 2016, p. 3 ss.

BACHMAIER WINTER L., *Criminal Investigation and Right of Privacy: the Case-law of the European Court of Human Rights and its Limits*, in *Lex ET Scientia International Journal*, 2009, 2, p. 12 ss.

BARATTA A., *Diritto alla sicurezza o sicurezza dei diritti?*, in S. Anastasia – M. Palma (a cura di), *La bilancia e la misura*, Milano, 2001, p. 22 ss.

BARBERA A., sub *Art. 2*, in G. Branca (a cura di), *Commentario della Costituzione. Principi fondamentali*, Bologna, 1975, p. 65 ss.

BARBERA A., *I principi costituzionali della libertà personale*, Milano, 1967

BARILE P. – CHELI E., voce *Domicilio (libertà di)*, in *Enc. dir.*, vol. XIII, Milano, 1964, p. 861 ss.

BARILE P. – CHELI E., voce *Corrispondenza (libertà di)*, *Enc. dir.*, vol. X, Milano, 1962, p. 743 ss.

BARILE P., *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984

BAROCCU G., *Le indagini sotto copertura*, Napoli, 2011

BARONA VILAR S., *Algoritmizaciòn del derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Valencia, 2021

BARRERA S., *Claves de la Investigaciòn en Redes Sociales*, Roquetas de Mar, 2016

BARTOLI L. – LASAGNI G., *The handling of digital evidence in Italy*, in M. Caianiello – A. Camon (a cura di), *Digital forensic evidence. Towards common european standards in antifraud administrative and criminal investigation*, Padova, 2021, p. 87 ss.

BARTOLI L., *Parità delle armi e* e-discovery *nel processo penale: quali indicazioni da Strasburgo*, in R. Brighi (a cura di), *Nuove questioni di informatica forense*, Roma, 2022, p. 83 ss.

BARTOLI L., *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. pen.* web., 5 marzo 2018

BASSINI M., Internet *e libertà di espressione. Prospettive costituzionali e sovranazionali*, Roma, 2019

BASSIOUNI M.C., *Introduction to the International Criminal Law*, Londra, 2003

BAUMAN Z., *Vita liquida*, Bari, 2006

BECCARIA C., *Dei delitti e delle pene*, (1764), Parigi, 1828

BEDI M., *The Curious Case of Cell Phone Location Data: Fouth Amendament Doctrine Mash-Up*, in *Northwestern University Law Review*, 2015, p. 61 ss.

BEDI M., *Social Network, Government Surveillance, and the Fourth Amendament Mosaic Theory*, in *Boston University Law Review*, 2014, p. 1809 ss.

BEDI M., *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should not Apply*, in *Boston College Law Review*, 2013, p. 1 ss.

BELLAVISTA G., *Studi sul processo penale*, vol. II, Milano, 1960

BELVINI L., *Principio di proporzionalità e attività investigativa*, Napoli, 2022

BENE T., *Il pedinamento elettronico: tecnica investigativa e tutela dei diritti fondamentali*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 443 ss.

BERLUSCONI G., *Social Network Analysis and Crime Prevention*, in B. Leclerc – E.U. Savona (a cura di), *Crime Prevention in the 21st Century. Insightful Approaches for Crime Prevention Initiative*, Cham, 2017, p. 129 ss.

BERRUTI L.V., Cyber terrorism*: esigenze di tutela preventiva e nuovi strumenti di contrasto*, in *Leg. pen.* web, 15 gennaio 2016

BESHEARS M.L., *Effectiveness of Police Social Media Use*, in *American Journal of Criminal Justice*, 2014, p. 489 ss.

BIN R., *Critica della teoria dei diritti*, Milano, 2018

BOBBIO N., *L'età dei diritti*, Torino, 1990

BOYD D., *Privacy and Publicity in the Context of Big Data*, 29 aprile 2010, in *https://www.danah.org/papers/talks/2010/WWW2010.html*

BONINI V., *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in *Proc. pen. giust*., 2019, p. 338 ss.

BONINI V., *Il sistema di protezione della vittima e i suoi riflessi sulla libertà personale*, Milano, 2018

BONTEMPELLI M., *Acquisizione di dati custoditi in ambiente* Cloud, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 589 ss.

BONTEMPELLI M., *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont.*, 20 dicembre 2018

BOS-OLLERMAN H., *Mass Surveillance and Oversight*, in D.D. Cole – F. Fabbrini – S. Schulhofer (a cura di), *Surveillance, Privacy and Trans-Atlantic Relations*, Oxford, 2017, p. 139 ss.

BOYD D.M. – ELLISON N.B., *Social Network Sites: Definition, History, and Scholarship*, in *Journal of Computer-Mediated Communication*, 2007, 13, p. 210 ss.

BREEN C., *Silent No More: How Deepfakes Will Force Courts to Reconsider Video Admission Standards*, in *The Journal of High Technology Law*, 1° giugno 2021

BRENNER S.W., *Encryption, Smart Phones, and the Fifth Amendment*, in *Whittier Law Review*, 2012, p. 525 ss.

BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen.*, 1967, p. 1079 ss.

BRONZO P., *L'impiego de*l trojan horse *informatico nelle indagini penali*, in *Rivista italiana di scienze giuridiche*, 2019, p. 347 ss.

BROWN I. – MARSDEN C.T., *Regulating Code. Good Governance and Better Regulation in the Information Age*, Cambridge-Londra, 2013

BROWNING J.G., *Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, in *Science and Technology Law Review*, 2017, p. 465 ss.

BROWNING J.G., *Why Can't We Be Friends? Judges' Use of Social Media*, in *University of Miami Law Review*, 2014, p. 487 ss.

BRUGNOLI G., *Della certezza e prova penale*, Modena, 1846

BRUNTY J. – HELENEK K., *Social Media Investigation for Law Enforcement*, New York, 2013

BUENO DE MATA F., *Investigación y prueba de delitos de odio en Redes Sociales: Técnicas OSINT e inteligencia policial*, Valencia, 2023

BUENO DE MATA F., *Las digilencia de investigacion penal en la cuarta revolucion industrial. Principios teoricos y problemas practicos*, Cizur Menor, 2019

BUENO DE MATA F., *Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*, in *Diario la Ley*, 19 ottobre 2015

BUENO DE MATA F., *Prueba Electrónica y Proceso 2.0*, Valencia, 2014

BUNGERT M., *Do it For the Snap: Different Methods of Authenticating Snapchat Evidence for Criminal Prosecutions*, in *University of Illinois Journal of Law, Technology & Policy*, 2021, p. 122 ss.

BYGRAVE L.A. – BING L., *Internet Governcance: Infrastructure and Insitution*, Oxford, 2009

BYRNE J. – MARX G., *Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact*, in *Journal of Police Studies*, 2011, p. 17 ss.

CABIALE A., *I limiti alla prova nella procedura penale europea*, Milano, 2019

CAIANIELLO M., *L'ammissione della prova scientifica nel processo penale italiano*, in G. Canzio – L. Lupária (a cura di), *Prova scientifica e processo penale*, Milano, 2022, p. 189 ss.

CAIANIELLO M., *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventinve Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2021, 29, p. 1 ss.

CAIANIELLO M., *Amissione della prova e contraddittorio nelle giurisdizioni penali internazionali*, Torino, 2008

CAJANI F., *Le "nuove frontiere" dell'investigazione digitale alla luce della legge n. 48/2008, ovvero: quello che le norme (ancora) non dicono*, in AA.VV., Cyber forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, p. 541 ss.

CAJANI F., *Le indagini informatiche per i reati di cyberterrorismo*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 1791 ss.

CALABRÒ V.G., *Mobile device and mobile cloud computing forensics*, Torino, 2016

CALAMANDREI P., *Verità e verosimiglianza nel processo civile*, in *Riv. dir. proc.*, 1955, p. 164 ss.

CALAMANDREI P., *Il giudice e lo storico*, in *Riv. dir. proc*., 1939, p. 105 ss.

CALDERA E., *Reject the Evidence of Your Eyes and Ears: Deepfakes and the Law of Virtual Replicants*, in *Seton Hall Law Review*, 2019, p. 3 ss.

CAMON A., *Sfondi*, in AA.VV., *Fondamenti di procedura penale*, Milano, 2020, p. 3 ss.

CAMON A., *Cavalli di troia in Cassazione*, in *Arch. n. proc. pen.*, 2017, p. 91 ss.

CAMON A., *La fase che "non conta e non pesa": indagini governate dalla legge*, in AA.VV., *Legge e potere nel processo penale*, Milano, 2017, p. 93 ss.

CAMON A., voce *captazione di immagini* (dir. proc. pen.), in *Enc. dir.*, Annali VI, Milano, 2013, p. 133 ss.

CAMON A., *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. proc. pen*., 2006, p. 1550 ss.

CAMON A., *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen*., 2005, p. 594 ss.

CAMON A., *La disciplina delle indagini genetiche*, in *Cass. pen*., 2014, p. 1426 ss.

CAMON A., *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, p. 1188 ss.

CAMON A., *Le intercettazioni nel processo penale*, Milano, 1996

CANESCHI G., *Il diritto a un processo equo*, in M. Ceresa-Gastaldo – S. Lonati (a cura di), *Profili di procedura penale europea*, Milano, 2023, p. 125 ss.

CANTONE R., sub *Art. 234-bis c.p.p*., in G. Canzio – R. Brichetti (a cura di), *Codice di procedura penale*, Milano, 2017, p. 1601 ss.

CANZIO G., *Un'efficace strategia comunicativa degli uffici giudiziari vs. il processo mediatico*, in *Dir. pen. proc.*, 2018, p. 1537 ss.

CAPOGRASSI G., *Giudizio, processo, scienza, verità*, in *Riv. dir. proc*., 1950, p. 1 ss.

CAPPELLETTI M., *Dimensioni della giustizia nelle società contemporanee*, Bologna, 1994

CAPRIOLI F., *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, in L. Lupária – L. Marafioti – G. Paolozzi (a cura di), *Dimensione tecnologica e prova penale*, Torino, 2019, p. 45 ss.

CAPRIOLI F., *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. Bras. de Direito Processual Penal*, 2017, p. 483 ss.

CAPRIOLI F., *Il giudice e la legge processuale: il paradigma rovesciato*, in *Ind. pen.*, 2017, p. 967 ss.

CAPRIOLI F., *Sicurezza dei cittadini e processo penale*, in M. Donini – M. Pavarini (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, p. 143 ss.

CAPRIOLI F., *Riprese visive nel domicilio e intercettazione "per immagini"*, in *Giur. cost*., 2002, p. 2176 ss.

CAPRIOLI F., *Colloqui riservati e prova penale*, Torino, 2000

CARBELLOTTO E., voce *Ricusazione ed astensione del giudice e degli ufficiali del pubblico ministero* (dir. proc. civ. e dir. proc. pen.), in *Enc. giur.*, vol. XIV, Milano, 1906, p. 363 ss.

CARLSON S., *When is a Tweet Not an Admissible Tweet? Closing the Authentication Gap in the Federal Rules of Evidence*, in *University of Pennsylvania Law Review*, 2016, p. 1033 ss.

CARNEVALE S., *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in D. Negri (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 3 ss.

CARRARA F., *Il diritto penale e la procedura penale. Prolusione al corso accademico di diritto penale dell'anno 1873-1874*, Lucca, 1873

CARTABIA M., *Le sentenze gemelle: diritti fondamentali, fonti, giudici*, in *Giur. cost*., 2007, p. 3564 ss.

CASSESE S., *Il diritto globale. Giustizia e democrazia oltre lo Stato*, Torino, 2009

CASTELLS M., *Communication, Power and Counter-power in the Network Society*, in *International Journal of Communication*, 2007, p. 238 ss.

CASTIELLO M., *Reti criminali.* Social network analysis *e* criminal intelligence analysis. *Tecniche di contrasto a confronto*, Roma, 2015

CECANESE G., *Le pre-investigazioni informatiche e i controlli sui* social, in A. Scalfati (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Torino, 2020, p. 267 ss.

CENTORAME F., *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. it. dir. proc. pen.*, 2021, p. 499 ss.

CERRINA FERONI G. – MORBIDELLI G., *La sicurezza: un valore superprimario*, in *Percorsi Costituzionali*, 2008, 1, p. 31 ss.

CESARI C., *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, 2019, p. 1167 ss.

CHALMERS D.J., *Più realtà. I mondi virtuali e i problemi della filosofia*, Milano, 2023

CHANDER A., *Facebookistan*, in *North Carolina Law Review*, 2012, p. 1807 ss.

CHELI E., *Conclusioni*, in *Osservatorio sulle fonti*, 2021, 2, p. 953 ss.

CHELO A., *Sequestro probatorio di strumenti di comunicazione: l'imprescindibilità di una riforma*, in *Dir. pen. proc.*, 2022, p. 1583 ss.

CHELO A., *Tutela della libertà morale e captatore informatico: è davvero tutto concesso a soddisfazione delle esigenze investigative?*, in *Dir. pen. proc*., 2022, p. 954 ss.

CHIAVARIO M., *Garanzie ed efficienza della giustizia penale. Temi e problemi*, Torino, 1998

CHIAVARIO M., *L'impatto delle nuove tecnologie tra diritti umani e interessi sociali*, in *Dir. pen. proc.*, 1996, p. 139 ss.

CHIAVARIO M., *Il processo penale dopo la nuova decretazione "d'emergenza": ancora una volta alla ricerca di una bussola*, in *Leg. pen*., 1993, p. 339 ss.

CHIAVARIO M., *Processo e garanzie della persona*, vol. II, Milano, 1984

CIPOLLA P., Social Network, *furto di identità e reati contro il patrimonio*, in *Giur. mer.*, 2012, p. 2672 ss.

CISTERNA A., *Cedu e diritto alla* privacy, in A. Gaito (a cura di), *I principi europei del processo penale*, Roma, 2016, p. 193 ss.

CISTERNA A., *All'Aise l'attività di informazione verso l'estero*, in *Guida dir*., 2015, 19, p. 95 ss.

CITRON D.K. – CHESNEY R., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, in *California Law Review*, 2019, p. 1753 ss.

CLOUD M., *Ignorance and Democracy*, in *Texas Tech Law Review*, 2007, p. 1143 ss.

COCCO G., *I servizi di informazione e sicurezza nell'ordinamento italiano*, Padova, 1980

CODELUPPI V., *La vetrinizzazione sociale*, Torino, 2007

COMELLA C., *Origine dei big data*, in *Rivista italiana di Intelligence*, 2017, p. 131 ss.

CONLY W.G., *Determining Relevancy: Article IV of the Federal Rules of Evidence*, in *Louisiana Law Review*, 1975, p. 70 ss.

CONSO G., *Sicurezza tra informazione, segreto e garanzie*, in *Per aspera ad Veritatem*, 1995, p. 27 ss.

CONSO G., *Macchine elettroniche e nuove prospettive giuridiche*, in *Riv. it dir. proc. pen.*, 1971, p. 660 ss.

CONTI C. – TORRE M., *Spionaggio digitale nell'ambito dei* social network, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 535 ss.

CONTI C., *Il principio di non sostituibilità: il sistema probatorio tra Costituzione e legge ordinaria*, in *Cass. pen.*, 2024, p. 451 ss.

CONTI C., *La prova scientifica alle soglie dei vent'anni dalla sentenza Franzese: vette e vertigini in epoca di pandemia*, in *Sist. pen.*, 9 febbraio 2021

CONTI C., *Sicurezza e riservatezza*, in *Dir. pen. proc.*, 2019, p. 1572 ss.

CONTI C., *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. proc.*, 2018, p. 1210 ss.

CONTI C., *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007

CONTI C., *Le videoriprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati"*, in *Dir. pen. proc.*, 2006, p. 1347 ss.

COOPER B.P., *Judges and Social Media: Disclosure as Disinfectant*, in *Science & Technology Law Review*, 2017, p. 521 ss.

CORDERO F., *Procedura penale*, Milano, 2012

CORDERO F., *Ideologie del processo penale*, Milano, 1966

CORDERO F., *Tre studi sulle prove penali*, Milano, 1963

CORNELI A., *Informazione e sicurezza. Il ruolo delle "fonti aperte"*, in *Rivista italiana di intelligence*, 2007, p. 25 ss.

CORRELL C.M., *Facebook, Crime Prevention, and the Scope of the Private Search Post-Carpenter*, in *Georgia Law Review*, 2022, p. 787 ss.

CORVI P., *Le modalità di acquisizione dei dati informatici trasmessi mediante posta elettronica e applicativi di* chatting: *un* rebus *non ancora del tutto risolto*, in *Proc. pen. giust.*, 2023, p. 216 ss.

COSTABILE G. – ATERNO S., *Le intercettazioni digitali*, in AA.VV., Cyber forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, p. 341 ss.

COSTABILE G., *Le indagini digitali*, in AA.VV., Cyber Forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, p. 61 ss.

COSTABILE G., *Rete* Internet *e "dintorni": aspetti tecnici di base*, in AA.VV., Cyber forensics *e indagini penali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, p. 33 ss.

COSTANZO P., *Aspetti evolutivi del regime giuridico di Internet*, in *Dir. inf. e informatica*, 1996, p. 785 ss.

CRISTIANI A., sub *Art. 38*, in *Commentario al nuovo codice di procedura* penale*. La normativa complementare*, coordinato da M. Chiavario, vol. I, Torino, 1989, p. 157 ss.

CROCKER T.C., *From Privacy to Liberty: The Fourth Amendament after Lawrence*, in *UCLA Law Review*, 2009, p. 1 ss.

CUOMO L., *La tutela penale del domicilio informatico*, in *Cass. pen.*, 2000, p. 2998 ss.

CURTOTTI D., *La sentenza costituzionale n. 170 del 2023 e le comunicazioni "apparenti": quando un eccesso di garanzie non sempre è un moltiplicatore di garanzie*, in *Dir. inf. e informatica*, 2023, p. 708 ss

CURTOTTI D., *"Le operazioni digitali sotto copertura": l'agente provocatore e l'attività di contrasto*, in AA.VV., Cyber Forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, p. 505 ss.

CURTOTTI D., *Indagini* hi-tech*, spazio* cyber*, scambi probatori tra Stati e* Internet provider service *e "Vecchia Europa": una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 2021, p. 745 ss.

CURTOTTI D., *Procedimento penale e* intelligence *in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Proc. pen. gust.*, 2018, p. 435 ss.

D'ALESSANDRA F. – SUTHERLAND K., *The Promise and Challenges of New Actors and New Technologies in International Justice*, in *Journal of International Criminal Justice*, 2021, p. 9 ss.

D'AMBROSIO L., *La pratica di polizia giudiziaria*, vol. I, Milano, 2007

D'AMBROSIO L., *Ruolo e attività della polizia giudiziaria nelle indagini: brevi considerazioni e qualche proposta*, in *Cass. pen*., 2006, p. 2685 ss.

DALIA A.A. – FERRAIOLI M., *Manuale di diritto processuale penale*, Padova, 2018

DAMAŠKA M.R., *What is the Point of International Criminal Justice?*, in *Chicago-Kent Law Review*, 2008, p. 329 ss.

DAMAŠKA M.R., *Il diritto delle prove alla deriva*, Bologna, 2003

DAMAŠKA M.R., *I due volti della giustizia e del potere. Analisi comparatistica del processo*, Bologna, 1991

DANIELE M., *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 1891 ss.

DANIELE M., *Ordine europeo di indagine penale e comunicazioni criptate: il caso* Sky ECC/Encrochat *in attesa delle Sezioni Unite*, in *Sist. pen.*, 11 dicembre 2023

DANIELE M., *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. Direito Processual Penal*, 2019, p. 1277 ss.

DANIELE M., *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. pen. giust*., 2018, p. 831 ss.

DANIELE M., *Le indagini informatiche contro il terrorismo bilanciamenti difficili e timori legislativi*, in R. Wenin – G. Fornasari (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, Trento, 2017, p. 265 ss.

DANIELE M., *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen*., 2013, p. 367 ss.

DANIELE M., *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 283 ss.

DAVARA FERNÁNDEZ DE MARCOS L., *Implicaciones Socio-Jurídicas de las Redes Sociales*, Cizur Menor, 2015

DE ARCOS TEJERIZO M., *Digital Evidence and fair trial rights at the International Criminal Court*, in *Leiden Journal of International Law*, 2023, p. 1 ss.

DE BUSSER E., *Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be USed Against You*, in *Groningen Journal of International Law*, 2014, p. 90 ss.

DE FILIPPI P. – MCCARTHY S., *Cloud Computing: Centralization and Data Sovereignity*, in *European Journal for Law and Technology*, 2012, p. 1 ss.

DE HERT P. – VAN LEEUW F., *Cybercrime Legislation in Belgium*, in E. Dirix – Y.-H. Leleu (a cura di), *The Belgian reports at the Congress of Washington of the International Academy of Comparative Law*, Bruxelles, 2011, p. 520 ss.

DE LEO F., *Il pubblico ministero tra completezza investigativa e ricerca dei reati*, in *Cass. pen*., 1995, p. 1431 ss.

DE MAGLIE C., *L'agente provocatore. Un'indagine dommatica e politico-criminale*, Milano, 1991

DEAN F., *Norma penale e territorio*, Milano, 1962

DEL COCO R., *L'utilizzo probatorio dei dati* whatsapp *tra lacune normative e avanguardie giurisprudenziali*, in *Proc. pen. giust.*, 2018, p. 532 ss.

DEL PIZZO A., *I crimini informatici a sfondo sessuale*, in M. Iaselli (a cura di), *Investigazioni digitali*, Milano, 2020, p. 421 ss.

DELGADO MARTIN J., *Investigacion tecnologica y prueba digital en todas las jurisdicciones*, Madrid, 2018

DELLA TORRE J., *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen*., 2022, p. 1057 ss.

DELLA TORRE J., *Ritratto di un'archiviazione come atto di (cripto)accusa*, in *Arch. pen.* web, 12 maggio 2021

DELLA TORRE J., *La giustizia penale negoziata in Europa. Miti, realtà e prospettive*, Milano, 2019.

DELLA TORRE J., *Il paradosso della direttiva sul rafforzamento della presunzione di innocenza e del diritto di presenziare al processo: un passo indietro rispetto alle garanzie convenzionali?*, in *Riv. it. dir. proc. pen.*, 2016, p. 1835 ss.

DEMOCKO B.M., *Social Media and the Rules on Authentication*, in *University of Toledo Law Review*, 2012, p. 367 ss.

DENARDIS L., *Internet in ogni cosa. Libertà, sicurezza e* privacy *nell'era degli oggetti iperconnessi*, Roma, 2022

DEUTH J. – HABAL H., *The Syrian Archive: A Methodological Case Study of Open Source Investigation of State Crime Using Video Evidence From Social Media Platforms*, in *State Criminal Journal*, 2018, p. 46 ss.

DI BITONTO M.L., *Raccolta di informazioni e attività di* intelligence, in R.E. Kostoris – R. Orlandi (a cura di), *Contrasto al terrorismo interno e internazionale*, Torino, 2006, p. 253 ss.

DI CHIARA G., *Atipicità e sistemi probatori: linee per una fenomenologia generale*, in V. Militello – A. Spena (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Torino, 2018, p. 371 ss.

DI CHIARA G., *Il canto delle sirene. Processo penale e modernità scientifico-tecnologica: prova dichiarativa e diagnostica della verità*, in *Criminalia*, 2007, p. 19 ss.

DI PAOLO G., *Nuove sfide tra terrorismo, sviluppo tecnologico e garanzie fondamentali: note introduttive*, in R. Wenin – G. Fornasari (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, Trento, 2017, p. 243 ss.

DI PAOLO G., voce *Prova informatica* (dir. proc. pen.), in *Enc. dir.*, Annali VI, Milano, 2013, p. 736 ss.

DI PAOLO G., "*Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2008

DIDDI A., *L'inviolabilità della segretezza delle comunicazioni*, in F.R. Dinacci (a cura di), *Processo penale e costituzione*, Milano, 2010, p. 268 ss.

DINACCI F.R., *I modi acquisitivi della messaggistica* chat *o* e-mail*: verso letture rispettose dei principi*, in *Arch. pen.* web, 2024

DINACCI F.R., *L'agente sotto copertura e reati contro la pubblica amministrazione: nuovi difetti e vecchi vizi*, in *Arch. pen.* web, 4 maggio 2020

DINACCI F.R., *Giudice terzo e imparziale quale elemento "presupposto" del giusto processo tra Costituzione e fonti sovranazionali*, in *Arch. pen.* web, 18 ottobre 2017

DINACCI F.R., *L'inutilizzabilità nel processo penale. Struttura e funzioni del vizio*, Milano, 2008

DINACCI F.R., *L'irrilevanza processuale delle registrazioni di conversazioni tra presenti*, in *Giur. it.*, 1994, p. 1 ss.

DOMINIONI O., sub *Art. 66-68*, in *Commentario del nuovo codice di procedura penale*, diretto da E. Amodio – O. Dominioni, Milano, 1989, p. 402 ss.

EDWARDS L. – URQUHART L., *Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?*, in *International Journal of Law and Information Technology*, 16 dicembre 2015

EVANS, V. *The Emoji Code. How Smiley Faces, Love Hearts and Thumbs Up Are Changing the Way We Communicate*, Londra, 2017

FABBRINI S., *Nuove tecnologie, potere e cambiamento sociale*, in *Studi di Sociologia*, 1984, 2, p. 135 ss.

FANCHIOTTI V., *La giustizia penale statunitense.* Procedure v. Antiprocedure, Torino, 2022

FANCHIOTTI V., voce *Agente sotto copertura*, in *Enc. dir.*, Annali VIII, Milano, 2015, p. 1 ss.

FANCHIOTTI V., *Struttura della Corte e fase delle indagini*, in Id. (a cura di), *La Corte penale internazionale. Profili sostanziali e processuali*, Torino, 2014, p. 93 ss.

FANUELE C., *La localizzazione satellitare nelle investigazioni penali*, Milano, 2019

FANUELE C., *Dati genetici e procedimento penale*, Padova, 2009

FASOLI M., *Contro lo strumentalismo tecnologico. Per una teoria analitica della prescrittività degli artefatti*, in *Sistemi intelligenti*, 2020, p. 223 ss.

FASOLI M., *Cacciatori (di informazioni) e prede (di trappole cognitive) nel* web 2.0*: una lettura cognitivo-evoluzionista dell'attrattività dei* social network, in *Sistemi intelligenti*, 2019, p. 395 ss.

FEENEY M., *Deepfake Laws Risk Creating More Problems Than They Solve*, in *Regulatory Transparency Project of the Federalist Society*, 1° marzo 2021

FELICIONI P., *Le ispezioni e perquisizioni di dati e sistemi*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 1583 ss.

FELICIONI P., *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. giust.*, 2016, p. 118 ss.

FELICIONI P., *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Milano, 2007

FERGUSON A.G., *Policing Predictive Policing*, in *Washington Law Review*, 2017, p. 1109 ss.

FERRAJOLI L., *Diritto e ragione. Teoria del garantismo penale*, Roma-Bari, 2004

FERRAIOLI M., *Il ruolo di «garante» del giudice per le indagini preliminari*, Padova, 2001

FERRAZZANO M. – SUMMA L., *La selezione dei dati informatici in ambito giudiziario: prassi e modalità applicative*, in R. Brighi (a cura di), *Nuove questioni di informatica forense*, Roma, 2022, p. 61 ss.

FERRER BELTRAN J., *Prova e verità nel diritto*, Bologna, 2004

FERRI E., *I nuovi orizzonti del diritto e della procedura penale*, Bologna, 1881

FERRUA P., *Il giusto processo*, Bologna, 2007

FERRUA P., *Studi sul processo penale*, vol. III, Torino, 1992

FERRUA P., *L'iniziativa del pubblico ministero nella ricerca della* notitia criminis, in *Leg. pen.*, 1986, p. 313 ss.

FILIPPI L., *Il cavallo di Troia e l'ispe-perqui-intercettazione*, in *PenaleDP*, 21 marzo 2022

FILIPPI L., *Ma davvero si può ricorrere a manovre fraudolente per intercettare col virus* trojan*?*, in *PenaleDP*, 9 febbraio 2021

FILIPPI L., *Le Sezioni unite decretano la morte dell'agente segreto "attrezzato per il suono"*, in *Cass. pen.*, 2004, p. 2094 ss.

FILIPPI L., *L'*home watching: *documento, prova atipica o prova incostituzionale?*, in *Dir. pen. proc.*, 2001, p. 92 ss.

FILIPPI L., *L'intercettazione di comunicazioni*, Milano, 1997

FIORELLI G., *Lo* screenshot *quale prova documentale: regole acquisitive e garanzie di affidabilità*, in *Dir. Internet*, 2020, p. 503 ss.

FIORINELLI G., Nomina nuda tenemus*? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche*, in *Discrimen*, 3 gennaio 2023

FISHER M. – BOLAND R. – LYYTINEN K., *Social Networking as the Production and Consumption of a Self*, in *Journal of Information and Organization*, 2016, p. 131 ss.

FLANAGAN E.A., *#Guilty: Sublet v. State and the Authentication of Social Media Evidence in Criminal Proceedings*, in *Villanova Law Review*, 2016, p. 287 ss.

FLEMING M.B. – WELLS J.T., *Ethical, Evidentiary, and Constitutional Concerns of Utilizing Social Networking Web Sites in Civil and Criminal Cases: the Good, the Bad, and the Ugly*, in *Southern Law Journal*, 2010, p. 23 ss.

FLETCHER D., *How Facebook is Redefining Privacy*, in *www.contenti.time.com*, 20 maggio 2010

FLEW T., *New media: An introduction*, Oxford, 2008

FLOR F., Phising, identity theft *e* identity abuse. *Le prospettive applicative nel diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, p. 899 ss.

FLORIAN E., *Principi di diritto processuale penale*, Torino, 1932

FLORIAN E., *Delle prove penali*, vol. II, Milano, 1924

FLORIDI L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017

FORLIVESI M., *Il controllo della vita del lavoratore attraverso i* social network, in P. Tullini (a cura di), Web *e lavoro. Profili evolutivi e di tutela*, Torino, 2017, p. 37 ss.

FOSCHINI G., *Il pubblico ministero in un processo penale a struttura giurisdizionale*, in *Justitia*, 1966, p. 38 ss.

FOX R.W., *The Return of "Vodoo Information": A Call to Resist a Heightened Authentication Standard for Evidence Derived From Social Networking Websites*, in *Catholic University Law Review*, 2013, p. 197 ss.

FREEMAN L. – VAZQUEZ LLORENTE R., *Finding the Signal in the Noise. International Criminal Evidence and Procedure in the Digital Age*, in *Journal of International Criminal Justice*, 2021, p. 163 ss.

FREEMAN L., *Digitally Disappeared: The Struggle to Preserve Social Media Evidence of Mass Atrocities*, in *Georgetown Journal of International Affairs*, 2022, p. 105 ss.

FREEMAN L., *Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court*, in S. Dubberley – A. Koenig – D. Murray (a cura di), *Digital Witness Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, Oxford, 2020, p. 432 ss.

FREEMAN L., *Law in Conflict. The Technological Transformation of War and its Consequences for the International Criminal Court*, in *International Law and Politics*, 2019, p. 807 ss.

FREEMAN L., *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, in *Fordham International Law Journal*, 2018, p. 283 ss.

FRIEDEN J.D. – MURRAY L.M., *The Admissibility of Electronic Evidence under the Federal Rules of Evidence,* in *Richmond Journal of Law and Technology*, 2011, 17, p. 1 ss.

FRIMAN H., *Procedures of International Criminal Investigations and Prosecutions*, in E. Cryer – H. Friman – D. Robinson – E. Wilmshurst (a cura di), *An Introduction to International Criminal Law and Procedure*, Cambridge, 2010, p. 465 ss.

FROSINI T.E., *Il costituzionalismo nella società tecnologica*, in *Dir. inf. e informatica*, 2020, p. 465 ss.

FROSINI T.E., *Il diritto costituzionale di accesso ad* Internet, in M. Pietrangelo (a cura di), *Il diritto di accesso ad Internet*, Napoli, 2011, p. 23 ss.

FROSINI V., *Cibernetica diritto e società,* Milano, 1968

FUENTES SORIANO O., *La impugnaciòn de la prueba digital,* in AA.VV., *Tendencias actuales del Derecho Procesal,* Valencia, 2019, p. 277 ss.

GABRIELLI C., *Il prelievo coattivo di campioni biologici nel sistema penale*, Torino, 2012

GAETA P., *Dichiarazioni dell'indagato "provocate" da agenti infiltrati: la libertà di autodeterminazione quale canone di utilizzabilità*, in *Cass. pen*., 2000, p. 967 ss.

GAITO A. – FURFARO S., *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, in A. Gaito (a cura di), *I principi europei del processo penale*, Roma, 2016, p. 363 ss.

GAITO A. – FURFARO S., *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen.*, 2016, p. 309 ss.

GALANTINI N., voce *Vizi degli atti processuali penali*, *Dig. disc. pen.*, vol. XV, Torino, 1999, p. 341 ss.

GALANTINI N., *L'inutilizzabilità della prova nel processo penale,* Padova, 1992

GALGANI B., *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Milano, 2022

GALGANI B., *Giudizio penale,* habeas data *e garanzie fondamentali*, in *Arch. pen.* web., 8 febbraio 2019

GALLO M., *Diritto penale e Costituzione*, in *Dir. pen. cont.*, 25 ottobre 2018

GANNON J., *The Strategic Use of Open Source Information*, in *Intelligence Community Persepctive*, 2014, p. 67 ss.

GARAPON A., *Lo Stato minimo. Il neoliberalismo e la giustizia*, Milano, 2012

GARCIA R. – HOFFMEISTER T.A., *Social Media Law in a Nutshell*, in *School of La Faculty Publication*, 2017, p. 1 ss.

GASCÓN INCHAUSTI F., *Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial*, in AA.VV., *La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro,* Barcellona, 2019, p. 191 ss.

GEBER M.S., *Predicting Crime using Twitter and kernel density estimation*, in *Decision Support Systems,* 2014, p. 115 ss.

GENTILE D.P., *Il diritto delle prove penali*, in E. Amodio – M.C. Bassiouni (a cura di), *Il processo penale negli Stati Uniti d'America*, Milano, 1988, p. 203 ss.

GEORGE C. – SCERRI J., *Web 2.0 and User-Generated Content: Legal Challenges in the New Frontier*, in *Journal of Information, Law and Technologies*, 2007, p. 4 ss.

GERBER M.S., *Predicting crime using Twitter and kernel density estimation*, in *Decision Support Systems*, 2014, p. 115 ss.

GIALUZ M. – DELLA TORRE J., *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022

GIALUZ M. – DELLA TORRE J., *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. cont.*, 2018, 5, p. 277 ss.

GIALUZ M., *Il giudizio di revisione*, in L. Lupária (a cura di), *L'errore giudiziario*, Milano, 2021, p. 567 ss.

GIALUZ M., *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 51 ss.

GIALUZ M., *Premessa*, in Id. (a cura di), *Le nuove intercettazioni. Legge 28 febbraio 2020 n. 7*, in *Dir. Internet*, 2020, Suppl. al n. 3, p. 1 ss.

GIALUZ M., *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Dir. pen. cont.*, 29 maggio 2019

GIALUZ M., *L'assistenza linguistica nel processo penale. Un meta-diritto fondamentale tra paradigma europeo e prassi italiana*, Padova, 2018

GIALUZ M., *L'apertura al sistema convenzionale muta gli equilibri e i connotati del giusto processo*, in *Dir. pen. proc.*, 2014, p. 8 ss.

GIALUZ M., *Radiologia e accertamenti medici coattivi: il difficile equilibrio tra libertà della persona ed esigenze di prova*, in *Riv. it. dir. proc. pen.*, 2012, p. 558 ss.

GIALUZ M., *La cooperazione informativa quale motore del sistema europeo di sicurezza*, in F. Peroni – M. Gialuz (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, p. 15 ss.

GIALUZ M., *Banche dati europee e procedimento penale italiano*, in F. Peroni – M. Gialuz (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, p. 235 ss.

GIARDA A., *Dichiarazioni autoaccusatorie "intercettate" in conversazioni e comunicazioni*, in *Corr. mer.*, 2007, p. 11 ss.

GIARDA A., *Un cammino appena iniziato*, in AA.VV., *Le indagini difensive. Legge 7 dicembre 2000, n. 397*, Milano, 2001, p. 5 ss.

GIARDA A., *Imparzialità del giudice e difficoltà operative derivanti dall'incompatibilità*, in AA. VV., *Il giusto processo*, Milano, 1998, p. 35 ss.

GIARDA A., *Persistendo 'l reo nella negativa*, Milano, 1980

GIARRUZZO M. – MARINI N., *Attività illecite su* Telegram: *la* social media intelligence *a supporto delle indagini*, in *Sicurezza e giustizia*, 21 luglio 2020

GILLESPIE A. – SHURSON J. – MASON S., *Encrypted data*, in S. Mason – D. Seng (a cura di), *Electronic Evidence and Electronic Signatures*, Londra, 2021, p. 397 ss.

GILLESPIE A., *Regulation of Internet Surveillance*, in *European Human Rights Law Review*, 2009, p. 552 ss.

GIOCOLI NACCI P., *Libertà di corrispondenza*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, vol. XII, Padova, 1990, p. 107 ss.

GIORDANO L., *Dopo le sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. pen. cont.*, 2017, 3, p. 177 ss.

GIOSTRA G., *La giustizia penale nello specchio deformante della cronaca giudiziaria*, in *Riv. dir. Media*, 2018, 3, p. 23 ss.

GIOSTRA G., *Processo penale e informazione*, Milano, 1989

GIUNCHEDI F., *Captazioni "anomale" di comunicazioni: prova incostituzionale o mera attività di indagine?*, in *Proc. pen. giust.*, 2014, 5, p. 133 ss.

GIUNCHEDI F., *Le attività di prevenzione e di ricerca di* intelligence, in A. Gaito (a cura di), *La prova penale*, vol. II, Torino, 2008, p. 1 ss.

GLADYSZ L.M., *Status Update: When Social Media Evidence Enters the Courtroom*, in *Journal of Law and Policy for the Information Society*, 2012, p. 691 ss.

GLANCY D.J., *Privacy on the Open Road*, in *Ohio Northern University Law Review*, 2004, p. 295 ss.

GOLDSMITH J.L., *Against Cyberanarchy*, in *University of Chicago Law Occasional Paper*, 1999, 40, p. 1199 ss.

GOLIN S., *Questioni aperte sull'acquisizione probatoria di dati informatici*, in R. Brighi (a cura di), *Nuove questioni di informatica forense*, Roma, 2022, p. 43 ss.

GOODFELLOW I.J. e altri, *Generative Adversarial Networks*, in *arXiv*, 2014

GORWA R. – BINNS R. – KATZENBACH C., *Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance*, in *Big Data & Society*, 2020, 7, p. 1 ss.

GRABOSKY P.N., *Virtual Criminality: Old Wine in New Bottles?*, in *Social & Legal Studies*, 2001, p. 243 ss.

GRAY D. – CITRON D.K., *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendament Privacy*, in *North Carolina Journal of Law and Technology*, 2013, p. 381 ss.

GREEN M.S., *The Privilege's Last Stand: the Privilege Against Self-Incrimination and the Right to Rebel Against the State*, in *Brooklyn Law Review*, 1999, p. 628 ss.

GREGORY S., *Ubiquitous Witnesses: Who Creates the Evidence and the Live(d) Experience of Human Rights Violations?*, in *Information, Communication & Society*, 4 agosto 2015

GREVI V., *Garanzie individuali ed esigenze di difesa sociale nel processo penale*, in L. Lanfranchi (a cura di), *Garanzie costituzionali e diritti fondamentali*, Roma, 1997, p. 255 ss.

GREVI V., *Funzioni di garanzia e funzioni di controllo del giudice nel corso delle indagini preliminari*, in AA.VV., *Il nuovo processo penale. Dalle indagini preliminari al dibattimento*, Milano, 1989, p. 15 ss.

GREVI V., *Ambiguità e limiti dell'uso del processo per fini di difesa sociale*, in G. Riccio (a cura di), *Dalle indagini preliminari alla sentenza di primo grado*, Napoli, 1979, p. 204 ss.

GREVI V., *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost*., 1973, p. 341 ss.

GREVI V., *Nemo tenetur se detegere: interrogatorio dell'imputato e diritto al silenzio nel processo penale italiano*, Milano, 1972

GREVI V., *Intercettazioni telefoniche e principi costituzionali*, in *Riv. it. dir. proc. pen*., 1971, p. 1064 ss.

GRIFFO M., *Il captatore informatico e la filosofia del doppio binario*, Napoli, 2019

GRIMM P.W. – BERGSTROM L. – O'TOOLE-LOUTERIO M.M., *Authentication of Social Media Evidence,* in *American Journal of Trial Advocacy,* 2013, p. 433 ss.

GRIMM P.W. – CAPRA D.J. – JOSEPH G.P., *Authenticating Digital Evidence*, in *Baylor Law Review*, 2017, p. 1 ss.

GRIMM P.W. – ZICCARDI M.V. – MAJOR A.W., *Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information*, in *Akron Law Review*, 2009, p. 357 ss.

GRIMM P.W., *Authenticating Digital Evidence*, in *GP Solo Magazine – American Bar Association*, 2014, 31, p. 47 ss.

GRIMMELMANN J., *Saving Facebook*, in *Iowa Law Review*, 2009, p. 1137 ss.

GUARIGLIA F., *"Admission" v. "Submission" of Evidence at the International Criminal Court*, in *Journal of International Criminal Court*, 2019, p. 315 ss.

GUERINI T., Fake news *e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Torino, 2020

HAFNER K. – LYON M., *La storia del futuro – Le origini di* Internet, Milano, 1998

HAKIM N., *How Social Media Companies Could Be Complicit in Incitement to Genocide*, in *Chicago Journal of International Law*, 2020, p. 83 ss.

HAMILTON R.J., *Social media Platforms in International Criminal Investigations*, in *Case Western Reserve Journal of Law*, 2020, p. 213 ss.

HAMILTON R.J., *User-Generated Content*, in *Columbia Journal of Transnational Law*, 2018, p. 1 ss.

HARAWA D.S., *Social Media Thoughtcrimes*, in *Pace Law Review*, 2014, p. 366 ss.

HASIBUAN E.S., *The Role of Indonesian Police Throught "Cyber Patrol" in Preserving and Mantaining Cyber Room Security*, in *International Journal of Social Service and Research*, 2022, p. 722 ss.

HIATT K., *Open Source Evidence on Trial,* in *Yale Law Journal Forum*, 2016, p. 323 ss.

HIGGINS E., *A New Age of Open Source Investigation: International Examples*, in B. Akhgar – P.S. Bayler – F. Sampson (a cura di), *Open Source Intelligence Investigation. From Strategy to Implementation*, Cham, 2016, p. 189 ss.

HOBBS C. – MORAN M. – SALISBURY D. (a cura di), *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities*, Londra, 2014.

HODGE M.J., *The Fourth Amendament and Privacy Issues on the New Interent: Facebook.com and Myspace.com*, in *Southern Illinois University of Law Journal*, 2006, p. 95 ss.

HOFFMEISTER T.A., *Liking the Social Media Revolution*, in *Science & Technology Law Review*, 2017, p. 507 ss.

HOFFMEISTER T.A., *Social Media in the Courtroom. A New Era for Criminal Justice?*, Santa Barbara, 2014

HOGAN B.W., *Griffin v. State: Setting the Bar Too High for Authenticating Social Media Evidence*, in *Maryland Law Review*, 2012, p. 61 ss.

HON W.K. – MILLARD C., *Cloud Technologies and Services*, in M. Millard (a cura di), *Cloud Computing Law*, Oxford, 2013, p. 1 ss.

HULNICK A., *The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?*, in J. Johnson (a cura di), *The Oxford Handbook of National Security Intelligence*, Oxford, 2010, p. 230 ss.

ILLUMINATI G., *La tutela della segretezza delle comunicazioni tra vecchio e nuovo codice*, in AA.VV., *Processo penale e valori costituzionali nell'insegnamento di Vittorio Grevi ad un anno dalla sua scomparsa*, Padova, 2013, p. 99 ss.

ILLUMINATI G., *Costituzione e processo penale*, in *Giur.it.*, 2008, p. 521 ss.

ILLUMINATI G., *La disciplina processuale delle intercettazioni*, Milano, 1983

ILLUMINATI G., *La presunzione di innocenza dell'imputato*, Bologna, 1979

IOVENE F., *Le c.d. perquisizioni on line tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont. – Riv. Trim.*, 2014, 3-4, p. 329 ss.

IOVENE F., *Perquisizione e sequestro di* computer: *un'analisi comparatistica*, in *Riv. dir. proc.*, 2012, p. 1607 ss.

IRVING E., *Suppressing Atrocity Speech on Social Media*, in *American Society of International Law*, 2019, p. 256 ss.

ITALIA V., *Libertà e segretezza della corrispondenza e delle comunicazioni*, Torino, 1963

JACKSON JONES M., *Shady Trick or Legitimate Tactic – Can Law Enforcement Officials Use Fictitious Social Media Accounts to Interact with Suspects*, in *American Journal of Trial Advocacy*, 2016, p. 69 ss.

JACOBS J., *I terroristi non hanno diritti*, in R.E. Kostoris – R. Orlandi (a cura di), *Contrasto al terrorismo interno e internazionale*, Torino, 2006, p. 3 ss.

JACOBSON Z.E., *Face Off: Overcoming the Fifth Amendment Conflict Between Cybersecurity and Self-Incrimination*, in *Journal of Law and Health*, 2023, p. 185 ss.

JALLOH C. – DI BELLA A., *Equality of Arms in International Criminal Law: Continuing Challenges*, in Y. Mcdermott – W.A. Schabas – N. Hayes (a cura di), *The Ashgate Research Companion to International Criminal Law-Critical Perspectives*, Londra, 2013, p. 251 ss.

JOHNSON B.R., *Untagging Ourselves: Facebook and the Law in the Virtual Panopticon*, in *Thomas M. Cooley Journal of Practical and Clinical Law*, 2011, p. 185 ss.

JOHNSON D.R. – POST D., *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, p. 1367 ss.

JONES E.N., *The Good and (Breaking) Dad of Deceptive Police Practices*, in *New Mexico Law Review*, 2015, p. 523 ss.

KALB L., *Il documento nel sistema probatorio*, Torino, 2000

KAPLAN A.M. – HEINLEIN M., *Users of the World, Unite! The Challenges and Opportunities of Social Media*, in *Business Horizons*, 2010, p. 59 ss.

KARAGIANNIS C. – VERGIDIS K., *Digital Evidence and Cloud Forenscs: Contemporary Legal Challenges and the Power of Disposal*, in *Information*, 22 aprile 2021

KERR O.S., *Compelled Decryption and the Privilege Against Self-Incrimination*, in *Texas Law Review*, 2018, p. 767 ss.

KERR O.S., *The Mosaic Theory of the Fouth Amendament*, in *Michigan Law Review*, 2012, p. 311 ss.

KERR O.S., *Digital Evidence and the New Criminal Procedure*, in *Columbia Law Review*, 2005, p. 279 ss.

KERR O.S., *Searches and Seizures in a Digital World*, in *Harvard Law Review*, 2005, p. 531 ss.

KERR O.S., *The Problem of Perspective in Internet Law*, in *Georgetown Law Journal*, 2003, p. 357 ss.

KOENIG A., *From 'Capture to Courtroom'. Collaboration and the Digital Documentation of International Crimes in Ukraine*, in *Journal of International Criminal Justice*, 2022, p. 829 ss.

KOENING A., *"Half the Truth is Often a Great Lie": Deep Fakes, Open Source Information, and International Criminal Law*, in *American Journal of International Law*, 19 agosto 2019

KOOPS B.J. – GOODWIN M., *Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law*, in *Tilburg Law School Research paper*, 2014, 5, p. 1 ss.

KOOPS B.J. – HOEPMAN J. – LEENES R., *Open Source Intelligence and Privacy by Design*, in *Computer Law and Security Review*, 2013, p. 676 ss.

KOOPS B.J., *Police Investigations in Internet Open Source: Procedural-Law Issues*, in *Computer Law & Security Review*, 2013, p. 654 ss.

KOSTORIS R.E., *Processo penale, diritto europeo e nuovi paradigmi del pluralismo giuridico postmoderno*, in *Riv. it. dir. proc. pen.*, 2015, p. 1177 ss.

KOSTORIS R.E., *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in F. Ruggieri – L. Picotti (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 179 ss.

KOSTORIS R.E., *Processo penale, delitto politico e «diritto penale del nemico»*, in *Riv. dir. proc.*, 2007, p. 1 ss.

KRISCH N., *Beyond Constitutionalism. The Pluralist Structure of Postnacional Law*, Oxford, 2010

LAMONAGA J.P., *A Break From Reality: Modernizing Authentication Standards for Digital Video Evidence in the Era of Deepfakes*, in *American University Law Review*, 2020, p. 1945 ss.

LASAGNI G., *AI-Powered Investigations: From Data Analysis to an Automated Approach Toward Investigative Uncertainty*, in L. Bachmaier Winter – S. Ruggeri (a cura di), *Investigating and Preventing Crime in the Digital Era. New Safeguards, New Rights*, Cham, 2022, p. 169 ss.

LASAGNI G., *Dalla riforma dei tabulati a nuovi modelli di integrazione fra diritti di difesa e tutela della* privacy, in *Leg. pen.* web, 21 luglio 2022

LASAGNI G., *La Corte di giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi (e la Corte costituzionale conferma)*, in *Giur. comm.*, 2021, p. 1179 ss.

LASAGNI G., *Tackling Phone Searches in Italy and the United States: Proposals for a Technological Rethinking of Procedural Rights and Freedoms*, in *New Journal of European Criminal Law*, 2018, p. 386 ss.

LASAGNI G., *L'uso di captatori informatici* (trojans) *nelle intercettazioni "fra presenti"*, in *Dir. pen. cont.*, 7 ottobre 2016

LEENES R., *Who controls the cloud?*, *Revista de Internet, derecho y política*, 2010, 11, p. 1 ss.

LESSING L., *Code And Other Laws of Ciberspace*, New York, 1999

LEVINSON-WALDMAN R., *Private Eyes, Thery're Watching You: Law Enforcement's Monitoring of Social Media*, in *Oklahoma Law Review*, 2019, p. 997 ss.

LEVINSON-WALDMAN R., *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, in *Howard Law Journal*, 2018, p. 525 ss.

LIDSKY L.B., *Public Forum 2.0*, in *Boston University Law Review*, 2011, p. 1975 ss.

LOGAN W.A. – LINFORD J., *Contracting for Fourth Amendament Privacy Online*, in *Minnesota Law Review*, 2019, p. 101 ss.

LONATI S., Predictive policing*: dal disincanto all'urgenza di un ripensamento*, in *Rivista diritto dei media*, 2022, 2, p. 302 ss.

LÒPEZ CABELLO A. – GRIFFA T.I., *Privacidad en redes sociales y vigilancia estatal: un desafio pendiente de la pràctica constitucional argentina*, in *Anuario de derecho consitutcional latinoamericano*, 2020, p. 793 ss.

LORUSSO S., *Investigazioni scientifiche, verità processuale ed etica degli esperti*, in *Dir. pen. proc.*, 2010, p. 1345 ss.

LORUSSO S., *Sicurezza pubblica e diritto emergenziale: fascino e insidie dei rimedi processuali*, in *Dir. pen. proc.*, 2010, p. 269 ss.

LOSAVIO D. – LOSAVIO M.M., *Prosecution and Social Media*, in C.D. Marcum – G.E. Higgins (a cura di), *Social Networking as a Criminal Enterprise*, Boca Raton, 2014, p. 199 ss.

LUPÁRIA L. – CERQUA F., *La versione della consulta sulla corrispondenza elettronica. Un* bouleversement *in materia di prova digitale?*, in *Dir. inf. e informatica*, 2023, p. 718 ss.

LUPÁRIA L., Privacy, *diritto della persona e processo penale*, in *Riv. dir. proc.*, 2019, p. 1448 ss.

LUPÁRIA L., *Il sistema penale ai tempi dell'*Internet. *La figura del provider tra diritto e processo*, in Id (a cura di), Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, p. 1 ss.

LUPÁRIA L., Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, diretto da G. Spangher, in G. Garuti (a cura di), *Modelli differenziati di accertamento*, t. I, Torino, 2011, p. 369 ss.

LUPÁRIA L., *La ratifica della convenzione* cybercrime *del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.*, 2008, p. 717 ss.

LUPÁRIA L., *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in L. Lupária – G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 141 ss.

LUPÁRIA L., *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in L. Lupária – G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 127 ss.

LUPÁRIA L., *Il caso "Vierika": un'interessante pronuncia in materia di* virus *informatici e prova penale digitale*, in *Dir. Internet*, 2006, p. 195 ss.

LUPÁRIA L., *La confessione dell'imputato nel sistema processuale penale*, Milano, 2006

LUTHER K. – HAYES R.M., *#Crime: Social Media, Crime and Criminal Justice*, New York, 2018

LYON D., *L'occhio elettronico.* Privacy *e filosofia della sorveglianza*, Milano, 1997

MAILLART J-B., *The Limits of Subjective Territorial Jurisdiction in the context of Cybercrime*, in *ERA Forum*, 2019, p. 375 ss.

MALACARNE A., *"Profundamente falso" y "profundamente incierto": el deepfake como* automated evidence *en el proceso penal. Consideraciones generales*, in *Revista General de Derecho procesal*, 2023, 60, p. 1 ss.

MALACARNE A., *La presunzione di non colpevolezza nell'ambito del d.lgs. 8 novembre 2021, n. 188: breve sguardo d'insieme*, in *Sist. pen.*, 17 gennaio 2022.

MALACARNE A., *Le registrazioni di colloqui ad opera di uno degli interlocutori tra contrasti interpretativi ed evoluzione tecnologica*, in *Dir. Internet*, 2021, p. 159 ss.

MANCUSO E.M., *L'acquisizione di contenuti* e-mail, in A. Scalfati (a cura di*), Le indagini atipiche*, Torino, 2019, p. 497 ss.

MANCUSO E.M., *L'ingresso dei* big data *nel procedimento penale*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*, Milano, 2019, p. 171 ss.

MANES V. – CAIANIELLO M., *Introduzione al diritto penale europeo. Fonti, metodi, istituti, casi*, Torino, 2020

MANGIARACINA A., *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici… e non solo*, in *Proc. pen. giust.*, 2021, p. 729 ss.

MANGIARACINA A., *Nuovi scenari nell'accesso transfrontaliero alla prova "elettronica"*, in V. Militello – A. Spena (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Torino, 2018, p. 421 ss.

MANN S. – NOLAN J. – WELLMAN B., *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, in *Surveillance & Society*, 2003, p. 331 ss.

MANTOVANI F., *Insicurezza e controllo della criminalità*, in *Riv. it. dir. proc. pen*., 2010, p. 1003 ss.

MANTOVANI G., *Informazione, giustizia penale e diritti della persona*, Napoli, 2011

MANZINI V., *Trattato di diritto penale italiano*, vol. V, in G.D. Pisapia (a cura di), *Delitti contro l'amministrazione della giustizia*, Torino, 1982

MANZINI V., *Trattato di diritto processuale penale italiano*, vol. I, Torino, 1925

MARAFIOTI L., Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4509 ss.

MARANDOLA A., *I registri del pubblico ministero tra notizia di reato ed effetti procedimentali*, Padova, 2001

MARAS M.H. – ALEXANDROU A., *Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos,* in *The International Journal of Evidence & Proof*, 2019, p. 255 ss.

MARCOLINI S., *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2015, 760 ss.

MARCOLINI S., *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche)*, in *Cass. pen*., 2010, p. 2855 ss.

MARCOLINI S., *Regole di esclusione costituzionali e nuove tecnologie*, in *Discrimen*, 2006, p. 387 ss.

MARINELLI C., *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007

MARMO M., Social media mining. *Estrarre e analizzare informazioni dai* social media, Milano, 2016

MARRAFFINO M., *La sostituzione di persona mediante furto di identità digitale*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrati – A. Manna – M. Papa, Milano, 2023, p. 321 ss.

MARTHEWS A. – TUCKER C.E., *The Impact of Online Surveillance on Behavior*, in D. Gray – S.E. Henderson (a cura di), *Cambridge Handbook of Surveillance Law*, Cambridge, 2017, p. 437 ss.

MARTIN RIOS P., *Digital forensics and criminal process in Spain: evidence gathering in a Changing context*, Cizur Menor, 2022

MARZADURI E., *Inviolabilità della difesa e trasformazioni del processo*, in D. Negri – L. Zilletti (a cura di), *Nei limiti della Costituzione. Il Codice Repubblicano e il processo penale contemporaneo*, Milano, 2019, p. 111 ss.

MARZADURI E., *Considerazioni sul significato dell'art. 27, comma 2, Cost.: regola di trattamento e regola di giudizio,* in F.R. Dinacci (a cura di), *Processo penale e Costituzione*, Milano, 2010, p. 303 ss.

MARZADURI E., *La parità delle parti nel processo penale*, in *Quad. cost.*, 2007, p. 378 ss.

MARZELL L., *OSINT as a Part of the Strategic National Security Landscape*, in B. Akhgar – P.S. Bayerl – F. Sampson (a cura di), *Open Source Intelligence Investigation. From Strategy to Implementation*, Cham, 2016, p. 35 ss.

MASSA F., Osint *e Cyber intelligence: tecniche di investigazione nella rete*, in *Sicurezza e giustizia*, 21 gennaio 2016

MAYER-SCHÖNBERGER V. – CUKIER K., *Big data. A Revolution That Will Transform How we Leave, Work and Think*, Oxford, 2014

MAZZA O., *Tradimenti di un codice. La procedura penale a trent'anni dalla grande riforma*, Torino, 2020

MAZZA O., *Presunzione d'innocenza e diritto di difesa*, in *Dir. pen. proc.*, 2014, p. 1401 ss.

MAZZA O., *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont. – Riv. Trim.*, 2013, 3, p. 4 ss.

MAZZA O., *Le persone pericolose (in difesa della presunzione d'innocenza)*, in *Dir. pen. cont*., 20 aprile 2012

MAZZA O., *Il garantismo al tempo del giusto processo*, Milano, 2011

MAZZA O., *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, Milano, 2004

MCDERMOTT Y. – KOENIG A. – MURRAY D., *Open Source Information's. Blind Spot Human and Machine Bias in International Criminal Investigations*, in *Journal of International Criminal Justice*, 2021, p. 85 ss.

MCDERMOTT Y. – MURRAY D. – KOENIG A., *Whose Stories Get Told, and by Whom? Representativeness in Open Source Human Rights Investigations*, in *www.opiniojuris.org*, 19 dicembre 2019

MCPARTLAND M.D., *An Analysis of Facebook "Likes" and Other Nonverbal Internet Communication Under the Federal Rules of Evidence*, in *Iowa Law Review*, 2013, p. 445 ss.

MEHANDRU N. – KOENIG A., *ICTS, Social media & the Future of Human Rights*, in *Duke Law & Technology Review*, 2019, p. 130 ss.

MEHANDRU N. – KOENIG A., *Open Source Evidence and the International Criminal Court*, in *Harward Human Rights Journal*, 15 aprile 2019

MEHLMAN J., *Facebook and MySpace in the Courtroom: Authentication of Social Networking Websites*, in *Criminal Law Brief*, 2012, p. 10 ss.

METZ H., *"Your Device is Disabled": How and Why Compulsion of Biometrics to Unlock Devices Should be Protected by the Fifth Amendament Privilege*, in *Valparaiso University Law Review*, 2019, p. 427 ss.

MILLER B., *Open Source Intelligence (OSINT): An Oxymoron*, in *International Journal of Intelligence and Counter Intelligence*, 2018, p. 702 ss.

MILLER C., *The Social Medium: Why the Authenticantion Bar Should Be Raised for Social Media Evidence*, in *Template Law Review Online*, 2014 p. 1 ss.

MILLER G.A., *Informavores*, in F. Machlup – U. Mansfield (a cura di), *The study of Information: Interdisciplinary Messages*, New York, 1986, p. 111 ss.

MINOTTI K., *The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, in *South Carolina Law Review*, 2009, p. 1057 ss.

MIRAGLIA M., *Il "*Trojan *(non) di Stato": una disciplina da completare*, in *Proc. pen. giust.*, 2023, p. 1227 ss.

MIRAGLIA M., *Diritto di difesa e giustizia penale internazionale*, Torino, 2011

MIRAGLIA M., *Garanzie costituzionali nel processo penale statunitense. Tendenze e riflessioni*, Torino, 2008

MODUGNO F., *I «nuovi diritti» nella Giurisprudenza Costituzionale*, Torino, 1995

MONTAGNA M., *Libertà domiciliare*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*, Milano, 2019, p. 119 ss.

MONTE M. – SÀNCHEZ S.I., *Tensiones constitucionales entre el derecho a la intimidad y el ciberpatrullaje en la investigación criminal. Análisis del Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas*, in *Revista pensamiento penal*, 23 aprile 2021

MONTI A., *La nuova disciplina del sequestro informatico*, in L. Lupária (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 197 ss.

MORELLI A. – POLLICINO O., *Le metafore della rete. Linguaggio figurato,* judicial frame *e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto*, in *Rivista AIC*, 2018, 1, p. 1 ss.

MORGESE G., *Moderazione e rimozione dei contenuti illegali* online *nel diritto dell'UE*, in *Federalismi.it*, 12 gennaio 2022

MORRONE A., *Il custode della ragionevolezza*, Milano, 2001

MOSCARINI P., *Il silenzio dell'imputato sul fatto proprio secondo la Corte di Strasburgo e nell'esperienza italiana*, in *Riv. it. dir. proc. pen.*, 2006, p. 611 ss.

MUMFORD L., *II mito della macchina*, Milano, 1969

MUND B., *Social Media Searches and the Resonable Expectation of Privacy*, in *Yale Journal of Law and Technology*, 2017, p. 238 ss.

MURPHIY J.P. – FONTECILLA A., *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, in *Richmond Journal of Law & Technologiy*, 2013, p. 1 ss.

MURRAY D. – MCDERMOTT Y. – KOENIG A., *Mapping the Use of Open Source Research in UN Human Rights Investigations*, in *Journal of Human Rights Practice*, 2022, p. 554 ss.

NEGRI D., *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, p. 3 ss.

NEGRI D., *Diritto costituzionale applicato: destinazione e destino del processo penale*, in *Proc. pen. giust.*, 2019, p. 553 ss.

NEGRI D., *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Arch. pen*., 2016, p. 44 ss.

NERONI REZENDE I., *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, in *New Journal of European Criminal Law*, 2020, p. 375 ss.

NICOLICCHIA F., *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Milano, 2020

NICOLICCHIA F., *Sorveglianza di massa e prerogative di riservatezza dell'individuo durante l'emergenza* SARS-CoV-2. *Scenari attuali e prospettive future*, in AA.VV., *Diritto virale: scenari e interpretazioni delle norme per l'emergenza* #Covid19, vol. I, Ferrara, 2020, p. 15 ss.

NICOLICCHIA F., *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Dir. pen. cont*., 8 gennaio 2018

NIETO MARTIN A. – MAROTO M., *Redes sociales en internet y "data mining" en la prosepcciòn e investigaciòn de comportamientos delictivos*, in *Revista de derecho penal y criminologia*, 2013, p. 1ss.

NOBILI M., *Scenari e trasformazioni del processo penale*, Padova, 1998

NOBILI M., *Principio di legalità e processo penale (ricordando Franco Bricola)*, in *Riv. it. dir. proc. pen.*, 1995, p. 648 ss.

NOBILI M., *Prove «a difesa» e investigazioni di parte nell'attuale assetto delle indagini preliminari*, in *Riv. it. dir. proc. pen.*, 1994, p. 398 ss.

NOBILI M., sub *Art. 189 c.p.p.*, in M. Chiavario (a cura di), *Commento al nuovo codice di procedura penale*, Vol. II, Torino, 1990, p. 399 ss.

NOBILI M., *La nuova procedura penale. Lezioni agli studenti*, Bologna, 1989

NOBILI M., *Atti di polizia amministrativa utilizzabili nel processo penale e diritto di difesa: una pronuncia marcatamente innovativa*, in *Foro it*., 1984, I, p. 375 ss.

NOCERINO W., *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Milano, 2021

NOCERINO W., *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, Milano, 2018

NORTH E., *Facebook Isn't Your Space Anymore: Discovery af Social Networking Websites*, in *Kansas Law Review*, 2010, p. 1279 ss.

NUVOLONE P., *Legalità penale, legalità processuale e recenti riforme*, in *Riv. it. dir. proc. pen.*, 1984, p. 3 ss.

NUVOLONE P., *Funzionamento e prospettive della giustizia penale in un mondo in evoluzione*, in *Ind. pen.*, 1983, p. 233 ss.

O'FLOINN M. – ORMEROD D., *Social Networking Material as Criminal Evidence*, in *Criminal Law Review*, 2012, p. 486 ss.

O'FLOINN M.– ORMEROD D., *Social Networking Sites, RIPA and Criminal Investigations*, in *Criminal Law Review*, 2011, p. 766 ss.

O'REILLY Y., *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, in *Communications & Strategies,* 2007, 1, p. 17 ss.

OMAND S.D. – BARTLET J. – MILLER C., *Introducing Social Media Intelligence (SOCMINT)*, in *Intelligence and National Security*, 2012, p. 1 ss.

ONG W.J., *Oralità e scrittura. Le tecnologie della parola*, Bologna, 1986

OPDERBECK D.W., *The Skeleton in the Hard Drive: Encryption and the Fifth Amendment*, in *Florida Law Review*, 2018, p. 883 ss.

ORLANDI R., *Uso poliziesco dell'intelligenza artificiale. L'insegnamento del* Bundesverfassungsgericht, in *Cass. pen.*, 2023, p. 2167 ss.

ORLANDI R., *La duplice radice della presunzione di innocenza*, in *Riv. it. dir. proc. pen*., 2022, p. 627 ss.

ORLANDI R., *Procedimento di prevenzione e presunzione di innocenza*, in D. Negri – L. Zilletti (a cura di), *Nei limiti della Costituzione. Il codice repubblicano e il processo penale contemporaneo*, Milano, 2019, p. 85 ss.

ORLANDI R., *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen*., 2018, p. 538 ss.

ORLANDI R., *La giustizia penale nel gioco di specchi dell'informazione*, in *Dir. pen. proc. – Riv. Trim.*, 2017, 3, p. 47 ss.

ORLANDI R., *Esistono davvero diritti inviolabili?*, in V. Fanchiotti – M. Miraglia (a cura di), *Il contrasto alla criminalità organizzata. Contributi di studio*, Torino, 2016, p. 265 ss.

ORLANDI R., *Osservazioni sul documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Arch. pen.* web, 25 luglio 2016

ORLANDI R., *Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali*, in AA.VV., *La giustizia penale preventiva. Ricordando Giovanni Conso*, Milano, 2016, p. 5 ss.

ORLANDI R., *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, p. 1133 ss.

ORLANDI R., *Sicurezza e diritto penale. Dialogo di un processualista italiano con la scuola di Francoforte*, in M. Donini – M. Pavarini (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, p. 91 ss.

ORLANDI R., *Attività di* intelligence *e diritto penale della prevenzione*, in G. Illuminati (a cura di), *Nuovi profili del segreto di Stato e dell'attività di* intelligence, Torino, 2010, p. 227 ss.

ORLANDI R., *La prolusione di Rocco e le dottrine del processo penale*, in *Criminalia*, 2010, p. 207 ss.

ORLANDI R., *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 129 ss.

ORLANDI R., *Trasformazione dello Stato e crisi della giustizia penale*, in M. Vogliotti (a cura di), *Il tramonto della modernità giuridica. Un percorso interdisciplinare*, Torino, 2008, p. 235 ss.

ORLANDI R., *Rito penale e salvaguardia dei galantuomini*, in *Criminalia*, 2006, p. 293 ss.

ORLANDI R., *Garanzie individuali ed esigenze repressive (ragionando intorno al diritto di difesa nei procedimenti di criminalità organizzata)*, in AA.VV., *Studi in ricordo di Giandomenico Pisapia*, vol. II, Milano, 2000, p. 545 ss.

ORLANDI R., *Il processo nell'era di* Internet, in *Dir. pen. proc*., 1998, p. 140 ss.

ORLANDI R., *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell*'inquisitio generalis?, in *Riv. it. dir. proc. pen*., 1996, p. 568 ss.

ORLANDI R., *Atti e informazioni della autorità amministrativa nel processo penale. Contributo allo studio delle prove extracostituite*, Milano, 1992

OROFINO M., *L'articolo 15 della Costituzione italiana: osservazioni sulla libertà e sulla segretezza delle comunicazioni ai tempi del* web *2.0*, in T.E. Frosini – O. Pollicino – E. Papa – M. Bassini (a cura di), *Diritti e libertà in* Internet, Milano, 2017, p. 193 ss.

OSSIAN K.L., *Social Media and the Law*, New York, 2022

PACE A., *Metodi interpretativi e costituzionalismo*, in *Quaderni costituzionali*, 2001, 1, p. 35 ss.

PACE A., *Problematica delle libertà costituzionali. Lezioni (Parte speciale – I)*, Padova, 1985

PACE A., *Art. 15 Cost.*, in A. Branca (a cura di), *Commentario alla Costituzione*, Bologna-Roma, 1977, p. 80 ss.

PADOVANI T., *Il crepuscolo della legalità nel processo penale. Riflessioni antistoriche sulle dimensioni processuali della legalità penale*, in *Ind. pen*., 1999, p. 527 ss.

PAGANO F.M., *La logica dei probabili. Per servire di teoria alle prove nei giudizi criminali*, Salerno, 1924

PANZAVOLTA M., *Intercettazioni e spazio di libertà, sicurezza e giustizia*, in F. Ruggieri – L. Picotti (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 67 ss.

PAPA A., *Espressione e diffusione del pensiero in* Internet. *Tutela dei diritti e progresso tecnologico*, Torino, 2009

PAPA M., *Brevi spunti sulle* Rules of Evidence, in E. Amodio – M.C. Bassiouni (a cura di), *Il processo penale negli Stati Uniti d'America*, Milano, 1988, p. 353 ss.

PARAVINI M., *La polizia, la sua riforma, la società aperta*, in D. Fondaroli (a cura di), *Nuove strategie di polizia per una "società aperta"*, Milano, 2011, p. 11 ss.

PARKER D., *Crime by Computer*, New York, 1976

PARLATO L., *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale,* in *Proc. pen. giust.,* 2020, p. 291 ss.

PARLATO L., *Le nuove disposizioni in materia di indagini difensive. Commento alla legge 7 dicembre 2000, n. 397*, Torino, 2001

PARODI C., VoIP, Skype *e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?,* in *Dir. pen. proc*., 2008, p. 1309 ss.

PARRAT F.S., *Redes sociales: Fenómeno pasajero o reflejo del nuevo internauta*, in *Cuadernos de comunicación e innovación*, 2008, p. 118 ss.

PASSAGLIA P., Privacy *e nuove tecnologie, un rapporto difficile. Il caso emblematico dei* social media, *tra regole generali e ricerca di una specificità*, in *Consultaonline.it*, 28 settembre 2016

PASSAGLIA P., Internet *nella Costituzione italiana: considerazioni introduttive*, in *Consultaonline.it*, 4 dicembre 2013

PATANÈ V., *Il diritto al silenzio dell'imputato*, Torino, 2006

PATRIKARAKOS D., *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty–First Century*, Londra, 2017

PATRONO P., voce Privacy *e vita privata* (dir. pen.), in *Enc. dir*., vol. XXXV, Milano, 1986, p. 557 ss.

PAULESU P.P., *Notizia di reato e scenari investigativi complessi: criminalità organizzata, indagini sotto copertura, captazione di dati digitali*, in *Riv. dir. proc*., 2010, p. 787 ss.

PAULESU P.P., *La presunzione di non colpevolezza dell'imputato*, Torino, 2009

PAULESU P.P., *Contrasto al terrorismo e presunzione di non colpevolezza*, in *Riv. dir. proc*., 2008, p. 623 ss.

PAYNE A.C., *Twitigation: Old Rules in a New Word*, in *Washburn Law Journal*, 2010, p. 845 ss.

PECORELLA C., *Diritto penale dell'informatica*, Padova, 2006

PELISSERO M., *Contrasto al terrorismo internazionale e il diritto penale al limite*, in *Quest. giust*., spec. 2016, p. 99 ss.

PENNEY J.W., *Chilling Effects: Online Surveillance and Wikipedia*, in *Berkeley Tech Law Journal*, 2016, p. 117 ss.

PEREIRA PUIGVERT S., *De vuelta con la aportación y valoración de la prueba electrónica de Whatsapp y su interpretación acorde con el contexto y el testimonio de la denunciante. Comentario de la Sentencia del Tribunal Supremo (Sala de lo Penal) 920/2021, de 24 de noviembre*, in *La Ley Probática*, 2022, 7.

PEREIRA PUIGVERT S., *Las medidas de investigación tecnológicas y su injerencia en la privacidad de las personas y la protección de datos personales*, in *Investigación y prueba en los procesos penales de España e Italia*, diretto da I. Villar Fuentes, Cizur Menor, 2019, p. 297 ss.

PEREZ ESCODA A. – DANS E., *La interacciòn social como mercancìa: redes sociales y plataformas*, in A. Perez Escoda – J. Rubio Romero (a cura di), *Redes Sociales ¿El quinto poder? Una aproximación por ámbitos al fenómeno que ha transformado la comunicación pública y privada*, Valencia, 2021, p. 23 ss.

PÉREZ-LUÑO ROBLEDO C.E., *El procedimiento de Habeas Data. El derecho procesal ante las nuevas tecnologías*, Madrid, 2017

PERKINS R.M., *The Territorial Principle in Criminal Law*, in *Hastings Law Journal*, 1971, p. 1155 ss.

PERLINGIERI C., *Profili civilistici dei* social networks, Napoli, 2014

PETRASHEK N., *The Fourth Amendament and the Brave New World of Online Social Networking*, in *Marquette Law Review*, 2010, p. 1494 ss.

PETRINI D., *La responsabilità penale per i reati via* Internet, Napoli, 2004

PFEFFERKORN R., *"Deepfakes" in the Courtroom*, in *Boston University Public Interest Law Journal*, 2020, p. 245 ss.

PHELPS L., *It Is Only Fingerprint: Biometric Compulsion and the Fifth Amendment*, in *UMKC Law Review*, 2020, p. 461 ss.

PICA G., *Diritto penale delle tecnologie informatiche*, Torino, 1999

PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme*, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 31 ss.

PICOTTI L., *La tutela penale della persona e le nuove tecnologie dell'informazione*, in Id. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 29 ss.

PICOTTI L., *I diritti fondamentali nell'uso ed abuso dei* social network. *Aspetti penali*, in *Giur. mer*., 2012, p. 2522 ss.

PICOTTI L., *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. econ*., 2011, p. 827 ss.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Id. (a cura di), *Il diritto penale dell'informatica nell'epoca di* Internet, Padova, 2004, p. 21 ss.

PISANI M., *La tutela penale della «riservatezza»: aspetti processuali*, in *Riv. it. dir. proc. pen.*, 1967, p. 785 ss.

PISAPIA G.D., *Introduzione*, in AA.VV., *Il codice di procedura penale. Esperienze, valutazioni, prospettive*, Milano, 1994, p. 26 ss.

PITTIRUTI M., *Dalla Corte di cassazione un* vademecum *sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali* omnibus, in *Sist. pen.*, 14 gennaio 2021

PITTIRUTI M., *L'impego processuale dei messaggi inviati mediante l'applicazione* Telegram *tra "scorciatoie" probatorie e massime di esperienza*, in *Dir. Internet*, 2020, p. 313 ss.

PITTIRUTI M., Digital evidence *e procedimento penale*, Torino, 2017

PIVATY A. e altri, *Opening Pandora's box: The Right to Silence in Police Interrogations and the Directive 2016/343/EU*, in *New Journal of European Criminal Law*, 2021, p. 328 ss.

POBLET M. – KOLIEB J., *Responding to Human Rights Abuses in the Digital Era: New Tools, Old Challenges*, in *Stanford Journal of International Law*, 2018, p. 277 ss.

POLLICINO O., voce *Potere digitale*, in *Enc. dir.*, vol. V, Milano, 2023, p. 410 ss.

POLLICINO O., *The Right To Internet Access*, in A. von Arnauld – K. von der Decken – M. Susi (a cura di), *The Cambridge Handbook of New Human Rights*, Cambridge, 2020, p. 263 ss.

POSTMAN N., *Technopoly. La resa della cultura alla tecnologia*, Torino, 1993

PROCACCINO A., *Piccoli equivoci senza importanza: tra intercettazioni di flussi informatici, perquisizioni e prove atipiche*, in *Cass. pen.*, 2022, p. 3112 ss.

PULITANÒ D., *Sui rapporti tra diritto penale sostanziale e processo*, in *Riv. it. dir. proc. pen.*, 2005, p. 951 ss.

PULVIRENTI A., *Campagne mediatiche e istanze di rimessione del processo*, in N. Triggiani (a cura di), *Informazione e giustizia penale. Dalla cronaca giudiziaria al processo mediatico*, Bari, 2022, p. 233 ss.

QUATTROCOLO S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020

QUATTROCOLO S., *Qualcosa di meglio del diritto (e del processo) penale?*, in F. Consulich – M. Miraglia – A. Peccioli (a cura di), *Alternative al processo penale? Tra deflazione, depenalizzazione,* diversion *e prevenzione*, Torino, 2020, p. 169 ss.

RATCLIFFE J., *Intelligence-Led Policing*, Cullompton, 2008

REITANO L., *Esplorare* Internet. *Manuale di investigazione digitale e* Open Source Intelligence, Bologna, 2014

RESTA G., *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Dir. inf. e informatica*, 2015, p. 23 ss.

RICCI G.F., *Le prove atipiche*, Milano, 1999

RICCIO G., *Politica penale dell'emergenza e Costituzione*, Napoli, 1982

RICOTTA F.N., *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'auto-incriminazione*, in *Cass. pen*., 2022, p. 880 ss.

RIFKIN J., *L'era dell'accesso, La rivoluzione della* new economy, Milano, 2000

RINCEANU J., V*erso una forma di polizia privata nello spazio digitale? L'inedito ruolo dei provider nella disciplina tedesca dei* social network, in *Sist. pen*., 11 marzo 2021

RIVA G., *I* social network, Bologna, 2016

ROBBINS I.P., *Writings on the Wall: The Need for an Autorship-Center Approach to the Autentication of Social-Networking Evidence*, in *Minnesota Journal of Law, Science and Technology*, 2012, p. 2 ss.

RODOTÀ S., *Elaboratori elettronici e controllo sociale*, 1973 (Ristampa anastatica a cura di G. Alpa), Napoli, 2018

RODOTÀ S., *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014

RODOTÀ S., *Il diritto di avere diritti*, Roma-Bari, 2012

RODOTÀ S., *Una Costituzione per* Internet, in *Politeia*, 2006, p. 177 ss.

RODOTÀ S., *La* privacy *tra individuo e collettività*, in *Pol. dir.*, 1974, p. 545 ss.

RODRÍGUEZ ÁLVAREZ A., *La «investigación viral»: una primera reflexión sobre el web sleuthing a partir del caso Gabby Petito*, in *Modernización, eficiencia y aceleración del proceso*, diretto da S. Pereira Puigvert – M.J. Pesqueira Zamora, Cizur Menor, 2022, p. 285 ss.

RODRÍGUEZ ÁLVAREZ A., *¿Sobran las palabras? Los emojis como prueba en el proceso judicial*, in *Revista de la Facultad de Derecho de México*, 2019, p. 675 ss.

RODRÍGUEZ ÁLVAREZ A., *Redes sociales y proceso penal: una radiografía*, in C. Alonso Salgado (a cura di), *El nuevo proceso penal sin Código Procesal Penal*, Barcellona, 2019, p. 321 ss.

RODRÍGUEZ ÁLVAREZ A., *Proceso penal y twitter: manual de instrucciones*, in *Propostas de modernización do dereito*, diretto da M. García Goldar – J. Ammerman Yebra, Santiago de Compostela, 2017, p. 111 ss.

RODRÍGUEZ RÍOS S.-F., *Una mirada al Reglamento (UE) 2021/784 como nuevo instrumento en la lucha contra la difusión del terrorismo en internet*, in *Investigación penal en el siglo XXI: nuevas tecnologías y protección de datos*, diretto da S. Pereira Puigvert – F. Ordóñez Ponz, Cizur Menor, 2021, p. 339 ss.

ROMANO R., *Innovazione giuridica e diritto tecnologico. L'impatto del giurista nei modelli di progresso sociale e scientifico*, in *Life Safety and Security*, 2017, p. 104 ss.

RUBECHI M., *Sicurezza, tutela dei diritti fondamentali e* privacy, in *Federalismi.it*, 30 novembre 2016

RUGGIERI F., *Profili processuali nelle investigazioni informatiche*, in L. Picotti (a cura di), *Il diritto penale dell'informatica nell'epoca di* Internet, Padova, 2004, p. 154 ss.

RUGGIERI F., *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001

RUGGIERI F., *La giurisdizione di garanzia nelle indagini preliminari*, Milano, 1996

RUOTOLO G.M., *Il ruolo del consenso del sovrano territoriale nel* transborder data access *tra obblighi internazionali e norme interne di adattamento*, in *La comunità internazionale*, 2016, p. 183 ss.

RUOTOLO G.M., Hey! You! Get Off My Cloud! *Accesso autoritativo alle nuvole informatiche e diritto internazionale*, in *Arch. pen.* web, 2013, p. 853 ss.

SABATINI G., *Principi di diritto processuale penale*, vol. I, Catania, 1948

SACCHETTO E., Face to face: *il complesso rapporto tra* automated facial recognition technology *e processo penale*, in *Leg. pen.* web, 16 ottobre 2020

SACHAROFF L., *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, in *Fordham Law Review*, 2018, p. 203 ss.

SAMMARCO P., *Giustizia e* social media, Bologna, 2019

SAMPSON F., *Following the Breadcrumbs: Using Open Source Intelligence as Evidence in Criminal Proceedings*, in B. Akhgar – P.S. Bayler – F. Sampson (a cura di), *Open Source Intelligence Investigation. From Strategy to Implementation*, Cham, 2016, p. 295 ss.

SANTI ROMANO, *Principii di diritto amministrativo italiano*, Milano, 1912

SCALFATI A., *Un ciclo giudiziario "travolgente"*, in *Proc. pen. giust.*, 2016, p. 113 ss.

SCAPARONE M., *Commento all'art. 24, secondo comma, Cost.*, in G. Branca (a cura di), *Commentario della Costituzione. Rapporti civili (artt. 24-26)*, Bologna, 1981, p. 54 ss.

SCAPARONE M., Common law *e processo penale*, Milano, 1974

SCHABAS W.A., *An Introducion to the Internatinal Criminal Court*, Cambridge, 2017

SCHABAS W.A., *The International Criminal Court. A Commentary on the Rome Statute*, Oxford, 2016

SCOTT J., *Social Network Analysis,* in *Sociology,* 1988, p. 109 ss.

SCOTT-HAYWARD C.S. – FRADELLA H.F. – FISCHER R.G., *Does Privacy Require Secrecy? Societal Expecttions of Privacy in the Digital Age*, in *American Journal of Crime Law*, 2015, p. 20 ss.

SEITZ N., *Transborder Search: A New Perspective in Law Enforcement?*, in *Yale Journal of Law and Technology*, 2005, p. 23 ss.

SEMINARA L., *Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani*, in *Rivista diritto dei media*, 2018, 2, p. 132 ss.

SEMITSU J.P., *From facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Government Surveillance*, in *Pace Law Review*, 2011, p. 291 ss.

SHOLL E.W., *Exhibit Facebook: The Discovery and Admissibility of Social Media Evidence*, in *Tulane Journal of Technology and Intellectual Property*, 2013, p. 207 ss.

SIEBER U. – NUEBERT C.-W., *Investigaciones transnacionales de crìmenes en el ciberspacio: retos a la sobranìa nacional*, in A. Nieto Martìn – B. Garcìa Moreno (a cura di), *Ius puniendi y Global Law. Hacia un dereho penal sin estado*, Valencia, 2019, p. 306 ss.

SIEBER U. – NEUBERT C-W., *Transnational Criminal Investigations in Cyberspace: Challenges to national sovereignty*, in *Max Planck Yearbook of United Nations Law,* 2017, p. 257

SIEBER U., *Legal Order in a Global Word. The Development of a Fragmented System of National, International, and Privat Norms*, in A. Von Bogdandy – R. Wolfrum (a cura di), *Max Planck Yearbook of United Nations Law*, 2010, 4, p. 1 ss.

SIGNORATO S., *Combating Terrorism on the Internet to Protect the Right to Life. The Regulation (EU) 2021/784 on Addressing the Dissemination of Terrorist Content Online*, in AA.VV., *Yearbook Human Rights Protection Right to Life*, Novi Sad, 2021, p. 403 ss.

SIGNORATO S., *Rimodulazioni normative dell'uso investigativo del captatore informatico*, in G. Giostra – R. Orlandi (a cura di), *Revisioni normative in tema di intercettazioni. Riservatezza, garanzie difensive e nuove tecnologie*, Torino, 2021, p. 319 ss.

SIGNORATO S., sub *Art. 234-bis c.p.p.*, in G. Illuminati – L. Giuliani (a cura di), *Commentario breve al Codice di procedura penale*, Milano, 2020, p. 988 ss.

SIGNORATO S., *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. proc.*, 2020, p. 605 ss.

SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018

SIGNORATO S., *Tipologie e caratteristiche delle* cyber investigations *in un mondo globalizzato*, in *Dir. pen. cont. – Riv. Trim.*, 2016, 3, p. 190 ss.

SIGNORATO S., *Le misure di contrasto in rete al terrorismo:* black list, *inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio* Internet, in R.E. Kostoris – F. Viganò (a cura di), *Il nuovo "pacchetto" antiterrorismo*, Torino, 2015, p. 55 ss.

SIGNORATO S., *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, p. 580 ss.

SILVESTRI G., *L'individuazione dei diritti della persona*, in *Dir. pen. cont.,* 29 ottobre 2018

SIMMONS R., *The Power and Pitfalls of Technology, Technology-Enhanaces Surveillance by Law Enforcment Officials*, in *NYU Annual Survey of American Law*, 2005, p. 711 ss.

SIRACUSANO F., *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione,* in *Proc. pen. giust.,* 2017, p. 178 ss.

SLOBOGIN C., *Domesic Surveillance of Public Activities and Transactions with Third Parties: Melding European and American Approaches*, in D.D. Cole – F. Fabbrini – S. Schulhofer (a cura di), *Surveillance, Privacy and Trans-Atlantic Relations*, Oxford, 2017, p. 31 ss.

SLOBOGIN C., *Public Privacy: Camera Surveillance fo public Places and the Right to Anonimity*, in *Mississipi Law Journal*, 2002, p. 13 ss.

SLOVE D.L. – SCHWARTZ P.M., *Privacy, Law Enforcement, and National Security*, Aspen, 2015

SORCI G., I social network. *Nuovi sistemi di sorveglianza e controllo sociale,* Palermo, 2015

SPANGHER G., *Ragionamenti sul processo penale*, Milano, 2018

SPANGHER G., *La rimessione dei procedimenti*, Milano, 1984

STANIFORTH A., *Police Use of Open Source Intelligence: The Longer Arm of Law*, in B. Akhgar – P.S. Bayler – F. Sampson (a cura di), *Open Source Intelligence Investigation. From Strategy to Implementation*, Cham, 2016, p. 21 ss.

STEEVES V., *Reclaiming the Social Value of Privacy*, in I. Kerr, V. Steeves y C. Lucock (a cura di), *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*, New York, 2009, p. 191 ss.

STELLA F., *Il giudice corpuscolano. La cultura delle prove*, Milano, 2005

STOYCHEFF E., *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, in *Journalism & Mass Communication Quarterly,* 2016, p. 296 ss.

SUGISAKA K.L., *Admissibility of E-Evidence in Minnesota: New Problems or Evidence as Usual?*, in *William Mitchell Law Review*, 2009, p. 1453 ss.

SVANTESSON D. – GERRY F., *Access to Extraterritorial Evidence: The Microsoft Cloud Case and Beyond*, in *Computer Law & Security Review*, 2015, p. 478 ss.

TARUFFO M., *La semplice verità. Il giudice e la costruzione dei fatti*, Bari, 2009

TARUFFO M., *Il giudice e lo storico: considerazioni metodologiche*, in *Riv. dir. proc*., 1967, p. 444 ss.

TAVORA SERRA M., *Ciberpatrullaje en el medio virtual. Delimitando conceptos,* in *Ius et Scientia,* 2023, p. 81 ss.

TELLO-DÍAZ L., *Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook,* in *Revista Cientifica de Comunicaciòn y Educaciòn*, 2013, p. 205 ss.

TEMPERINI M., *Delitos informàticos y cibercimen: tècnicas y tendencias de investigaciòn penal y su afectaciòn a los derechos constitucinales,* in D. Dupuy – J. Corvalàn (a cura di), *Cibercrimen III,* Montevideo, 2020, p. 219 ss.

TEN HULSEN L. , *Open Sourcing Evidence From The Internet – The Protection of Privacy In Civilian Criminal Investigations Using OSINT (Opens-Source Intelligence)*, in *Amsterdam Law Forum*, 11 giugno 2020

TESCONO M., Big data *e* social media intelligence, in *Rivista italiana di intelligence*, 2017, p. 106 ss.

THOMPSON J.J., *The Right to Privacy*, in *Philosophy and Public Affairs*, 1975, p. 295 ss.

TONINI P. – CONTI C., *Manuale di procedura penale*, Milano, 2023

TONINI P. – CONTI C., *Il diritto delle prove penali*, Milano, 2014

TONINI P., *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 401 ss.

TONINI P., *L'investigazione difensiva e la legge sulla* privacy, in L. Filippi (a cura di), *Processo penale: il nuovo ruolo del difensore*, Padova, 2001, p. 517 ss.

TONINI P., *Polizia giudiziaria e magistratura. Profili storici e sistematici*, Milano, 1979

TORRE M., Open source intelligence*: spionaggio digitale e* social network, in *Cybercrime*, diretto da A. Cadoppi – S. Canestrari – A. Manna – M. Papa, Milano, 2023, p. 1708 ss.

TORRE M., Privacy *e indagini penali*, Milano, 2020

TORRE M., Whatsapp *e l'acquisizione processuale della messaggistica istantanea*, in *Dir. pen. proc.*, 2020, p. 1279 ss.

TORRE M., *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017

TOSONI L., *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, in *Computer Law & Security Review*, 2018, p. 1197 ss.

TRAPELLA F., *Equo processo e inutilizzabilità tra codice e C.E.D.U.*, in *Arch. pen.*, 2020, p. 761 ss.

TRIGGIANI N., *Le investigazioni difensive*, Milano, 2002

TROGU M., *Intrusioni segrete nel domicilio informatico*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, p. 567 ss.

TROISI P., *Le investigazioni digitali sotto copertura*, Bari, 2022

TROISI P., *Dati PNR e trattamento pre-investigativo*, in A. Scalfati (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Torino, 2020, p. 319 ss.

TROTTIER D., *Coming to Terms with Social Media Monitoring. Uptake and Early Assessment*, in *Crime Media Culture*, 2015, p. 531 ss.

TROTTIER D., *Open Source Intelligence, Social Media and Law Enforcment: Visions, Constraints and Critiques*, in *European Journal of Cultural Studies*, 2015, p. 530 ss.

TROTTIER D., *Social Media as Surveillance: Rethinking Visibility in a Converging World*, Londra, 2012

TURÉGANO MANSILLA I., *La dimensión social de la privacidad en un entorno virtual*, in AA.VV., *Era digital, sociedad y derecho*, Valencia, 2020, p. 27 ss.

UBERTIS G. – PALTRINIERI V., *Intercettazioni telefoniche e diritto umano alla privatezza nel processo penale*, in *Riv. it. dir. proc. pen.*, 1979, p. 593 ss.

UBERTIS G., *Sisifo e Penelope. Il nuovo codice di procedura penale dal progetto preliminare alla ricostruzione del sistema*, Torino, 1993

UBERTIS G., *Variazioni sul tema dei documenti*, in *Cass. pen.*, 1992, p. 2516 ss.

VACIAGO G., Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012

VALASTRO A., *Libertà di comunicazione e nuove tecnologie. Inquadramento costituzionale e prospettive di tutela delle nuove forme di comunicazione interpersonale*, Milano, 2001

VASSALLI G., *Il diritto alla libertà morale*, in *Scritti giuridici*, vol. III, *Il processo e la libertà*, Milano, 1997, p. 306 ss.

VELE A., *Aspetti critici del documento probatorio "*screenshot*" e acquisito mediante il captatore informatico*, in *Arch. pen.* web, 8 marzo 2024

VENTURA N., *Le investigazioni* under cover *della polizia giudiziaria*, Bari, 2008

VERGANI M., *L'impatto della tecnologia digitale sulla sociologia visuale: opportunità e sfide*, in *Studi di Sociologia*, 2009, 4, p. 491 ss.

VIGANÒ F., *Terrorismo, guerra e sistema penale*, in *Riv. it. dir. proc. pen.*, 2006, p. 648 ss.

VINCENT JONES S., *Judges, Friends, and Facebook: The Ethics of Prohibition,* in *Georgetown Journal of Legal Ethics*, 2011, p. 286 ss.

VIOLA BERRUTI L., Black list *e blocco dei contenuti* web *illeciti: dal contrasto alla pedopornografia al* cyber terrorism, in *Leg. pen.* web, 15 gennaio 2016

VOENA G.P., *Processo mediatico e "mass media": il passato e il presente*, in *Leg. pen.* web, 19 ottobre 2020, p. 155 ss.

VOGLIOTTI M., voce *Legalità*, in *Enc. dir.*, Annali IX, Milano, 2013, p. 373.

WALDEN I., *Accessing Data in the Cloud: the Long Arm of the Law Enforcment Agent*, in *Queen Mary School of Law Legal Studies Research*, 10 marzo 2015.

WALDEN I., *Computer Crimes and Digital Investigations*, Oxford, 2007

WALDMAN A.E., *Privacy, Sharing, and Trust: The Facebook Study*, in *Case Western Reserve Law Review*, 2016, p. 193 ss.

WARKEN C., *Classification of Electronic Data for Criminal Law Purposes*, in *Eucrim*, 2018, 4, p. 1 ss.

WARR M., *Companions in Crime: The Social Aspects of Criminal Conduct*, Cambridge, 2002

WARREN S.D – BRANDEIS L.D., *The Right to Privacy*, in *Harward Law Review*, 1890, 4, p. 193 ss.

WIENER N., *La cibernetica*, Milano, 1953

WILSON J.S., *MySpcace, Your Space, or Our Space? New Frontiers in electronic Evidence*, in *Oregon Law Review*, 2007, p. 1201 ss.

WITNOV S., *Investigating Facebook: The Ethics of Using Social Networking Websites in Legal Investigations*, in *Santa Clara Computer Law & High Technology Law Journal*, 2011, p. 31 ss.

WOODS A.K., *Against Data Exceptionalism*, in *Standfor Law Review*, 2016, p. 729 ss.

ZACCHÈ F., *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 2013, p. 103 ss.

ZACCHÈ F., *La prova documentale*, Milano, 2012

ZANON N., *Un diritto fondamentale alla sicurezza?*, in *Dir. pen. proc.*, 2019, p. 1555 ss.

ZAPPALÀ E., *Il principio di tassatività dei mezzi di prova nel processo penale*, Milano, 1982

ZAPPULLA A., *La formazione della notizia di reato. Condizioni, poteri ed effetti*, Torino, 2012

ZARAGOZA TEJADA J., *Ciberpatrullaje e investigación tecnológica en la red. Una aproximación a la inteligencia artificial desde el punto de vista de la investigación y represión de hechos ilícitos*, in

Cibercrimen III: inteligencia artificial, automatización, algoritmos y predicciones en el derecho penal y procesal penal, coordinato da M. Kiefer, Buenos Aires, 2020, p. 209 ss.

ZENO-ZENCOVICH V., *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Rivista di diritto dei media*, 2018, 2, p. 32 ss.

ZICCARDI G., *Diritti digitali. Informatica giuridica per le nuove professioni*, Milano, 2022

ZICCARDI G., *La procedura di analisi della fonte di prova digitale*, in L. Lupária – G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 63 ss.

ZICCARDI G., *Scienze forensi e tecnologie informatiche*, in L. Lupária – G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 3 ss.

Avvertenze sulla giurisprudenza

Le sentenze della Corte di cassazione, dei Tribunali di merito, del Consiglio di Stato e dei Tribunali amministrativi regionali citate nel testo, salva diversa specificazione presente in nota, sono state reperite nelle banche dati *Dejure* o *Leggid'Italia*.

Le sentenze della Corte costituzionale citate nel testo sono state reperite sul sito ufficiale della Corte (*www.cortecostituzionale.it*).

Le sentenze delle Corti straniere citate nel testo sono state reperite nei siti ufficiali dei singoli Uffici giudiziari di rifermento.