La tutela dei diritti fondamentali nel contesto cibernetico. Profili di diritto interno, internazionale e dell'Unione europea

Indice

Capitolo 3

Il diritto alla libera espressione nell'era cibernetica e gli strumenti per tutelare la libertà di parola nel web

Capitolo 4

La privacy nell'epoca digitale: un bilanciamento tra interessi contrapposti per un'efficace tutela giurisdizionale e normativa del diritto alla riservatezza e all'autonomia informativa

Introduzione

L'avvento di Internet e delle nuove tecnologie di comunicazione è alla base di un profondo mutamento della società attuale sotto molteplici punti di vista; economico, culturale e giuridico. La circolazione delle informazioni sta acquisendo un ruolo sempre più fondamentale nel mondo contemporaneo, apportando rilevanti cambiamenti alla struttura tradizionale dei meccanismi produttivi; si affermano infatti nuovi metodi di organizzazione delle attività economiche e imprenditoriali, come la cd. *collaborative economy*, che erano francamente impensabili fino a pochi anni fa e che sono invece resi

possibili dall'incessante progresso tecnologico. Le informazioni sono diventate il nucleo centrale del ciclo economico, rappresentandone allo stesso tempo sia un mezzo produttivo che il risultato finale[1]. Sono difatti utilizzate dalle aziende e dalle industrie per produrre beni e servizi sempre più finalizzati a rispondere alle specifiche esigenze di ogni singolo individuo. Lo scopo è quello di fornire un'esperienza quanto più personalizzata possibile a ogni singolo cliente. Considerato ciò, i dati dei potenziali clienti diventano loro stessi dei prodotti che le aziende sono disposte a comprare, al fine di orientare le proprie produzioni. La pervasività e la diffusione globale di Internet, per non parlare della relativa economicità con cui è possibile accedervi, hanno reso il mondo "più piccolo" facendo sì che le distanze tra le persone diventassero sostanzialmente irrilevanti e non creassero più alcuno ostacolo alla comunicazione: questo ha permesso nuove forme di aggregazione sociale e politica.

Si pensi a tal proposito al ruolo fondamentale che i *social media* come Twitter o Facebook hanno avuto nell'epoca della cd. *Primavera Araba*[2], connettendo tra loro i cittadini e favorendo la diffusione delle loro idee di protesta in maniera tale da evitare le maglie della censura governativa.

I cambiamenti appena accennati, che verranno adeguatamente approfonditi nel corso dello studio, hanno importanti conseguenze anche nel contesto giuridico. Il rapido e costante progresso tecnologico sta creando non pochi problemi al mondo del diritto che si vede costretto a mettere in discussione tradizionali categorie giuridiche che non rispecchiano più una società in continua evoluzione. La "sfida" attuale per i legislatori nazionali e sovranazionali è perciò quella di regolamentare in maniera efficace l'ambiente informatico, tenendo ben presente le peculiari caratteristiche che questo ha e che lo contraddistinguono dalla realtà concreta quotidiana. Lo spazio cibernetico offre infatti importanti opportunità per lo sviluppo del singolo individuo e per l'intera società, ma pone anche dei rischi che non devono essere assolutamente sottovalutati.

Possibili effetti positivi come un'economia ecologicamente sostenibile, nuovi strumenti per supportare la creatività e l'estro artistico di ogni persona, la diffusione a livello globale di informazioni, educazione e sapere, l'inclusione del singolo cittadino nella formazione della coscienza pubblica e politica globale sono infatti controbilanciati

[1] G.SARTOR, *Human rights in the information society: utopias, dystopias and human values*, in (a cura di) M.V.DE AZEVEDO CUNHA, N.N.G.DE ANDRADE, L.LIXINSKI, L.T.FETEIRA, *New Technologies and Human Rights. Challenges to Regulation*, Burlington, 2013, pp.11-27.

[2] Si fa riferimento alla serie di proteste popolari anti-governative che ha caratterizzato la maggior parte dei Paesi nord africani e medio-orientali negli anni dal 2010 al 2012.

da rischi quali la perdita della propria riservatezza digitale e autonomia informativa, così come l'interferenza artificiale nel processo elettorale.

Occorre domandarsi quali possibilità ha l'essere umano, inteso sia come singolo individuo che come intera società, di regolamentare l'utilizzo delle nuove tecnologie, e in particolare di Internet, in maniera tale da prevenire suddetti rischi e quali strumenti ha concretamente a disposizione?

Per rispondere a questi quesiti occorre tenere in considerazione diversi aspetti che possono comportare competenze di non poco conto. La pervasività diffusa della rete cibernetica non tiene conto di confini politici, andando a coinvolgere in maniera simultanea un numero indefinito di ordinamenti normativi. Come si avrà modo di studiare nel proseguimento della trattazione, lo spazio cibernetico si caratterizza inoltre per concedere ai propri utenti un ampio spazio di autoregolamentazione; dove non è ancora arrivato il legislatore statale, i singoli cibernauti così come i *big players* dell'industria informatica contribuiscono a formare una sorta di autoregolamentazione del mondo virtuale. La volontà di sottoporre la realtà cibernetica ad un'unica disciplina normativa coerente e uniforme si scontra quindi con la contemporanea coesistenza di una pluralità indefinita di regolamentazioni provenienti da ordinamenti nazionali e sovranazionali, di origine pubblica o privata, che crea un "puzzle" giuridico di difficile soluzione.

Una completa regolamentazione dello spazio cibernetico rischia inoltre di profilarsi come uno sforzo titanico a causa dei numerosi aspetti da prendere in considerazione; rilevano infatti problematiche relative a diritti fondamentali quali la tutela della privacy e dell'autonomia informativa, la salvaguardia della libertà di espressione, ma anche aspetti più propriamente economici come l'*e-commerce*. I governi nazionali devono compiere perciò precise scelte politiche per individuare la direzione verso cui regolamentare il *cyberspace*.

Considerato che attendere il completo accordo di tutti gli attori della comunità internazionale su ogni aspetto relativo ad una possibile disciplina uniforme dello spazio cibernetico potrebbe rivelarsi alquanto utopistico, occorre ricorrere ad altri strumenti di regolamentazione. A tal proposito, proprio i diritti fondamentali potrebbero fornire delle linee guida sufficientemente articolate per una disciplina del ciberspazio che tenga conto dei valori umani in gioco[3]. In mancanza di una normativa strutturata che copra ogni aspetto dell'utilizzo di Internet e delle nuove tecnologie nel contesto globale attuale, i

[3] G.SARTOR, *op.cit.*

diritti fondamentali identificano una serie di bisogni umani non trascurabili, fornendo inoltre un efficace quadro di insieme per analizzare le nuove problematiche della società di informazione, facendo riferimento a categorie giuridiche di ormai comprovata efficacia. In altre parole, tali diritti trovano spazio anche nella realtà cibernetica e potrebbero essere la chiave giuridica per capire appieno la rilevanza del nuovo ambiente informatico.

Partendo da questo presupposto, il presente studio vuole proporre un'articolata analisi sui diritti fondamentali nel contesto cibernetico e sui più efficaci strumenti posti a loro tutela, siano essi di natura pubblica o internazional-privatistica. L'obbiettivo finale di questo lavoro è di individuare degli elementi giuridici attorno ai quali possa essere possibile costruire una regolamentazione del *cyberspace* strutturalmente uniforme e che tenga conto delle peculiari caratteristiche che contraddistinguono l'ambiente virtuale. Nel frattempo sarà inoltre possibile enucleare gli strumenti necessari per garantire agli internauti una proficua "navigazione" nel *mare magnum* virtuale e che rispetti i diritti inalienabili dell'essere umano.

Per raggiungere questi ambiziosi obbiettivi, si è voluto sviluppare un ragionamento che andasse a toccare alcuni diritti particolarmente rilevanti nel contesto cibernetico. L'attenzione si è concentrata in particolar modo sul diritto al libero accesso a Internet, sul diritto alla privacy e alla protezione dei dati personali e sul principio della libera espressione. La decisione di trattare in particolar modo questi precisi aspetti della vita digitale di ciascun cibernauta è data da diversi fattori. Si vuole dimostrare che gli specifici diritti presi in considerazione sono indissolubilmente collegati tra loro e possono (devono) essere quindi analizzati in maniera unica ed uniforme. Non è possibile parlare di libera espressione senza garantire la privacy di chi vuole affermare la propria idea. L'accesso a Internet funziona evidentemente come *conditio sine qua non*; non può esserci libertà di idee nello spazio cibernetico se si è impossibilitati ad accedere a tale dimensione. Questo legame a doppio filo deve caratterizzare l'approccio politico e legislativo in questo settore; lo studio vuole infatti dimostrare che l'unica scelta efficiente per garantire un quadro normativo alla dimensione cibernetica deve passare da una visione di insieme che tenga in considerazione gli interessi e i diritti di ogni singolo *stakeholder*. Si è scelto di prendere in considerazione questi specifici diritti anche per gli accadimenti che hanno acceso i riflettori del dibattito politico internazionale su tale materia: gli scandali Snowden e *Cambridge Analytica* sono solo gli ultimi avvenimenti che hanno sottolineato ancor di più l'esigenza impellente di maggiori tutele per la privacy

e la libertà di espressione in Internet. L'analisi vuole affiancare a uno studio normativo e giurisprudenziale delle modalità di tutela dei diritti fondamentali nel campo cibernetico anche alcune considerazioni di carattere culturale e sociologico.

Il Diritto è d'altronde una creazione umana che vuole rispondere alle esigenze di una società in continuo mutamento: per capire appieno il significato e la funzione dei principi esaminati occorre perciò avere contezza del contesto in cui tali norme sono state formulate. Per quanto concerne l'analisi degli strumenti normativi utilizzati nel contesto del *cyberspace* per la tutela delle prerogative fondamentali degli utenti virtuali, la prospettiva adottata vuole coinvolgere il quadro giuridico di diritto internazionale e dell'Unione europea alla luce della dimensione sovranazionale che ha la rete Internet. Senza alcuna pretesa di esaustività verranno però presi in considerazione anche alcuni profili di diritto interno che si contraddistinguono per la particolare novità o il significato impatto che hanno avuto nella successiva attività di regolamentazione.

L'analisi giurisprudenziale si è concentrata sui pronunciamenti della Corte di giustizia dell'Unione europea e sulla Corte europea dei diritti dell'uomo per diversi motivi. La prima ragione è di ordine meramente pratico, data dalla volontà di concentrare gli sforzi di ricerca su un ambito delimitato e poter quindi ricavare delle indicazioni dal materiale ricavato. Le sentenze prese in esame inoltre, per la loro carica innovativa e per i principi espressi, hanno avuto una particolare influenza politica e giuridica che ha travalicato i confini dell'Unione europea.

Prima di valutare gli strumenti normativi atti a tutelare tali principi, occorre però riflettere sul concetto stesso di *cyberspace*: la prima parte della tesi studia le caratteristiche ontologiche dello spazio virtuale, riflettendo sulla sua effettiva governabilità. Il secondo capitolo introduce il diritto all'accesso a Internet: tale principio, non ancora universalmente riconosciuto avente rango di diritto fondamentale, riveste però una particolare importanza permettendo agli individui di entrare nello spazio cibernetico e di non dover sopportare un pesante oblio digitale. Il terzo capitolo affronta il tema della libertà di espressione nel mondo virtuale: le nuove tecnologie di comunicazione hanno permesso a ciascun soggetto di far sentire la propria voce in ogni angolo del globo, rivoluzionando il tradizionale meccanismo di circolazione delle informazioni. Queste novità hanno importanti conseguenze anche nella formazione della coscienza pubblica e politica, influenzando i risultati elettorali delle moderne democrazie.

Considerato ciò, occorre riflettere su quali limiti abbia la libertà di parola in Internet e su cosa occorre fare per impedire che questa possa ledere la reputazione e la

dignità delle persone coinvolte. Strettamente collegato a questo quesito è quanto si va a trattare nel quarto e ultimo capitolo, ossia il diritto alla privacy e all'autonomia informativa nella realtà cibernetica. La continua e perdurante connessione a Internet, caratterizzata da un costante flusso senza riposo di dati e informazioni in ogni angolo del globo, ha annullato ogni spazio di riservatezza per l'essere umano. Non è più possibile invocare il diritto "ad essere lasciati soli", così come veniva intesa la privacy al momento della sua formulazione originaria, dato che non è rimasto alcuno spazio vitale in cui poter usufruire di una completa solitudine dalla società umana. Occorre invece chiedersi come la persona possa essere consapevole di quali dati che la riguardano stiano attualmente circolando nella realtà cibernetica e quali diritti possa effettivamente vantare su di essi.

Al termine della trattazione, si sarà auspicabilmente in grado di vedere le interconnessioni tra i diritti presi effettivamente in considerazione e di come, per una loro effettiva tutela, occorra un approccio globale e uniforme e non un'azione a compartimenti stagni; risulta impraticabile salvaguardare l'autonomia informativa di una persona senza considerare i limiti della libera espressione di un altro soggetto, e viceversa. Così come è impossibile considerare questi aspetti se le persone non possono godere di un effettivo accesso a Internet.

Prima di giungere a queste conclusioni e di formulare le dovute osservazioni in merito alla regolamentazione del *cyberspace* e alla tutela dei diritti fondamentali in esso rilevanti, occorre comprendere appieno cosa sia questo spazio cibernetico e quali siano le sue caratteristiche fondamentali in tema di governabilità e gestione.

Capitolo 1

La governabilità del ciberspazio e la tutela dei diritti fondamentali nel contesto virtuale

Sommario: 1. Un nuovo territorio virtuale e la sua struttura di governo - 1.1. Una definizione di cyberspace e del suo rapporto con la rete internet e il world wide web. - 1.2. Il concetto di governance del ciberspazio e la sua evoluzione geo-politica. - 1.3. I regimi legali dei territori tradizionali come esempio per la governabilità del ciberspazio. - 1.3.1. La potestà governativa dei singoli Stati nell'alto mare. - 1.3.2. Lo spazio profondo e gli altri corpi celesti come territori indipendenti e non sovrani. - 1.3.3. Lo status giuridico dell'Antartide. - 1.4. Nuove modalità di governo per un nuovo territorio come il cyberspace. - 1.4.1. Il ruolo dei privati nella governance dello spazio cibernetico: un approccio multilaterale a livello statale o una gestione partecipata "dal basso"? - 1.4.2. Una struttura di governo per il cyberspace. - 1.5. Il controllo militare sullo spazio cibernetico. - 2. Riflessioni conclusive. Autorità, extraterritorialità e giurisdizione nel cyberspace.

1. Un nuovo territorio virtuale e la sua struttura di governo: la gestione del ciberspazio e la tutela dei diritti fondamentali

1.1. Una definizione di cyberspace e del suo rapporto con la rete internet e il world wide web

Per comprendere al meglio quale struttura di governo possa essere adatta per il mondo virtuale, occorre specificare cosa si intenda con la parola ciberspazio e secondo quali norme e criteri questo ambiente possa essere gestito, pur essendo caratterizzato, per sua intrinseca natura, da una totale assenza di confini politici e giuridici entro i quali un Paese possa far valere la propria esclusiva giurisdizione e la propria potestà legislativa. Il dibattito sulla governabilità del ciberspazio è relativamente recente, considerata anche la giovane età del nuovo territorio virtuale; lo scontro si è acceso quando sono risultate evidenti le potenzialità che questa dimensione tecnologica poteva offrire, sia in termini di mezzo di comunicazione che di strumento per gli scambi commerciali.

Lo spazio cibernetico si inserisce in una realtà ancora più complessa, insieme alla rete internet e al *world wide web*, costruendo insieme a tali strumenti una rete interconnessa di reciproci scambi e relazioni.

Il sistema informatico viene comunemente suddiviso in tre diversi livelli[4]: il primo è caratterizzato dalle infrastrutture fisiche, il secondo dalle infrastrutture logiche e per ultimo quello in cui sono racchiusi i contenuti. Il primo comprende gli strumenti necessari alla connessione Internet, come cavi, *router* e *server*, mentre il secondo include i *software* necessari alla navigazione informatica[5] ed il terzo le informazioni condivise in rete. Non è semplice individuare in quali di questi livelli è possibile includere il *cyberspace*, considerando inoltre come queste classificazioni non siano da intendere come rigide demarcazioni.

Considerata questa prima suddivisione, è necessario spendere alcune parole sulla struttura della rete Internet e sulle sue caratteristiche peculiari. La natura eterogenea e la complessità dell'*hardware* che regge tale rete è descritta e testimoniata dalla sua struttura stratificata: Internet non è infatti un mondo omogeneo[6], ma è invece composto da piani separati e distinti[7]. Occorre perciò comprendere tale struttura al fine di governarla e regolamentarla al meglio; l'opera di governo deve essere diretta verso il preciso strato o livello che presenta l'aspetto problematico da risolvere nel caso concreto.

Uno dei principi fondamentali della progettazione della rete internet è la cd. *end-to-end architecture*, con cui si intende la sua natura decentralizzata e la sua indipendenza da un sistema centrale di distribuzione. Questa particolare architettura informatica dipende infatti da strumenti e accorgimenti[8] quali il *packet switching*; i vari *computer* e *device* connessi alla rete sono gestiti in maniera indipendente, ma fanno riferimento a un comune standard che permette loro di comunicare (protocollo TCP/IP). Il suddetto standard permette di suddividere i dati e le informazioni trasmesse in pacchetti che, dopo essere transitati tramite la rete Internet, vengono nuovamente assemblati nel computer a cui erano stati originariamente inviati. I dati, nel loro viaggio informatico, possono seguire qualsiasi percorso accessibile senza che la strada scelta influisca in alcun modo sulla velocità o qualità della trasmissione. Questa particolare caratteristica deriva dalla

---

[4] Y.BENKLER, *From consumers to users, shifting the deeper structures of regulation toward sustainable commons and user access*, in *Federal Communications Law Journal*, n.52, 2000, pp.561-562.
[5] L.LESSIG, *The Architecture of Innovation, Inaugural Meredith and Kip Frey Lecture in Intellectual Property at Duke University School of Law*, in *Duke Law Journal*, 2002, pp.1783-1786.
[6] L.LESSIG, *Code 2.0*, New York, 2006.
[7] L.B.SOLLUM, M.CHUNG, *The layers principle: internet architecture and the Law'*, in *Notre Dame Law Review*, vol.79 issue 3,https://scholarship.law.nd.edu/cgi/viewcontent.cgi?referer=http://scholar.google.it/&httpsredir=1&article=1432&context=ndlr (consultato il 7.7.2018).
[8] M.FROOMKIN, *The internet as a source of regulatory arbitrage*, in (a cura di) B.KAHIN, C.NESSON, *Borders in cyberspace*, Cambridge, 1996, pp.129-163.

volontà del primo utente di Internet, ossia il Ministero della Difesa statunitense, di far sì che il *network* resistesse a qualsiasi mancanza delle linee di comunicazione[9].

Dirette conseguenze del *packet switching* sono l'anonimità e la codificazione crittografica; un vario grado di anonimato è infatti garantito agli utenti del *web*. Sfruttando queste potenzialità, la rete può evadere da regimi regolatori restrittivi per compiere le proprie trasmissioni di informazioni sotto disposizioni più permissive[10]; si comprende perché risulta complesso censurare ciò che appare e viene diffuso nel ciberspazio. Ad esempio, un sito può essere registrato sotto diversi e disparati nomi di dominio, così come i contenuti informativi possono essere diffusi attraverso i servizi di *hosting*[11] disponibili. Internet si rivela essere un mezzo di comunicazione più liberamente accessibile e meno sottoponibile a censure dei *media* tradizionali; i Paesi che tentano, con diverso e alterno successo, di limitare la libera espressione e manifestazione del pensiero nel ciberspazio devono affrontare costi sempre maggiori all'incrementare della base di utenza e delle connessioni alla rete[12].

Ulteriore elemento da introdurre nella presente analisi, e che sarà oggetto di un'approfondita riflessione più avanti, è la cd. neutralità della rete[13]. Tale terminologia vuole indicare le modalità con cui Internet distribuisce i contenuti e le informazioni diffuse per via virtuale. Per ottenere una rete neutrale, occorre che gli *Internet Service Providers* (ISPs) non operino alcuna discriminazione tra i contenuti e i servizi offerti. Gli standard di prestazione (ad esempio la velocità della connessione, la sua stabilità, il suo costo etc.) dovrebbero essere gli stessi indipendentemente dalle applicazioni usate e dai contenuti effettivamente forniti. Gli operatori del settore, ritenendola un possibile ostacolo alle loro fonti di guadagno, auspicano di poter offrire servizi diversificati ai diversi utenti, a seconda del prezzo corrisposto da questi ultimi. Il dibattito sulla neutralità della rete è acceso e caratterizzato da posizioni politiche distinte e contrapposte, ma vi è certezza e unanimità di vedute sul fatto che questo tema caratterizzerà l'effettiva

[9] A.SAVIN, *Eu internet law*, Cheltenham, 2012, pp.3 ss.
[10] M.FROOMKIN, *op.cit.*, p.142.
[11] Un servizio di rete che consiste nell'allocare su un *server* un determinato sito o un singolo contenuto informativo, al fine di renderlo disponibile per tutta la platea degli utenti informatici.
[12] J.GOLDSMITH, T.WU, *Who controls the internet: illusions of a borderless world*, Oxford, 2006.
[13] D.NUNIZATO, *Virtual freedom: net neutrality and free spech in the internet age*, Stanford, 2009; T.W.HAZLETT, *The fallacy of net neutrality*, New York, 2011; A.STROVEL, *Net neutrality in Europe*, Bruxelles, 2013; K.MANADIAKI, *Eu competition law, regulation and the internet; the case of net neutrality*, Alphen aan den Rijn, 2015; L.BELLI, P.DE FILIPPI, *Net neutrality compendium; human rights, free competion and the future of internet*, Cham, 2016; C.T.MARSDEN, *Network neutrality: from policy to law to regulation*, Manchester, 2017.

governance dello spazio cibernetico e la concreta tutela dei diritti fondamentali nel mondo virtuale.

La neutralità della rete è diretta conseguenza dell'architettura informatica basata sul principio *end-to-end* a cui si faceva prima riferimento; il protocollo descrive come le macchine debbano comunicare tra loro, ma cosa debba essere inserito nella rete è una decisione che spetta ai singoli utenti. Cambiare l'equilibrio tra questi due profili, ossia incidere sulla effettiva neutralità del *network,* potrebbe danneggiarne il corretto sviluppo e l'armonia dello spazio cibernetico.

Per comprendere appieno la realtà del *cyberspace,* occorre introdurre anche il concetto di *web.* Sin dai suoi esordi nel 1989[14], il *world wide web* si è evoluto da un semplice sistema di ipertesti informatici usato da pochi esperti e professionisti del settore a un mezzo di comunicazione usato ogni giorno da milioni di persone. Nel solo territorio dell'Unione europea, nell'anno 2014, il 76% delle abitazioni aveva il proprio accesso a Internet, e il 70% della popolazione tra i 16 e i 74 anni affermava di connettersi *on-line* almeno una volta al giorno[15]. Il *web* presenta delle differenze significative rispetto alla rete Internet; la principale è che la seconda permette la connessione di diversi *computer* e la condivisione tra questi di dati e informazioni, mentre il *world wide web* consiste in un *network* di ipertesti reso accessibile attraverso una connessione informatica[16].

La parola ciberspazio viene spesso usata come sinonimo di Internet, ma invece ha caratteristiche e particolarità più ampie e differenziate. Il termine *cyberspace* venne utilizzato per la prima volta dallo scrittore di fantascienza William Gibson nel suo racconto *Burning Chrome,* pubblicato nel 1982 sulla rivista *Omni,* in contrapposizione a *meatspace*, letteralmente "spazio della carne", utilizzato dallo stesso scrittore per indicare il mondo della realtà fisica e concreta. Ciberspazio deriva a sua volta dalla fusione di due diverse parole, ossia cibernetica e spazio. La prima, coniata dallo scienziato Norbert Wiener[17], vuole indicare uno studio matematico unitario degli organismi viventi e di sistemi sia naturali che artificiali. Una possibile definizione[18] di questa nuova dimensione

---

[14] Lo scienziato britannico Tim Berners-Lee inventò il *web* al laboratorio *CERN* di Ginevra, https://home.cern/topics/birth-web (consultato il 12 luglio 2018).

[15] Eurostat (2015), Information, Society, Statistics. http://ec.europa.eu/eurostat/statistics-explained/index.php/ Information_society_statistics_-_households_and_individuals/de (consultato il 12 luglio 2018)

[16] J.KING, R.E.GRINTER, J.M.PICKERING, *The rise and fall of Netville: The saga of a cyberspace construction Boomtown in the great divide*, in (a cura di) S.Kiesler, *Culture of the internet,* 1997, Londra, pp.3-34.

[17] N.WIENER, *La cibernetica: controllo e comunicazione nell'animale e nella macchina*, Cambridge, 1948.

[18] La definizione di *cyberspace* in questione viene data dall'Oxford English Dictionary, http://www.oed.com/view/Entry/240849?redirected (consultato il 20 giugno 2018).

cibernetica è di spazio della realtà virtuale, dove avviene la comunicazione di informazioni e dati attraverso via elettronica. L'Organizzazione Internazionale per la Normazione (ISO) ha definito[19] lo spazio cibernetico come un ambiente risultante dall'interazione tra persone, *software* e servizi presenti su Internet, che avviene attraverso l'utilizzo di strumenti tecnologici e che non esiste in alcuna forma fisica.

Il termine ciberspazio introduce un ulteriore 'spazio' da sovrapporre alla dimensione fisica quotidiana, con nuovi livelli di informazioni raggiungibili attraverso strumenti quali la geolocalizzazione di persone, lo scambio di strumenti e flussi di dati. In questa nuova dimensione è possibile "navigare" (κυβερνήτης in greco antico indica il pilota di una nave; è evidente la somiglianza con il moderno termine cibernauta, ossia colui che si muove nel ciberspazio), sperimentando nuove modalità di relazione con la realtà circostante. I tentativi di mappare lo spazio cibernetico[20], creando una sorta di cartografia di questa dimensione alternativa, non sono riusciti a rendere in maniera completa le numerosissime interconnessioni di dati e informazioni che la popolano e la contraddistinguono. Nemmeno i motori di ricerca, novelli Virgilio tecnologici e automatizzati, riescono nell'intento di guidare l'utente in qualsiasi anfratto del ciberspazio, fornendone quindi una completa visione di insieme. La dimensione virtuale si presenta perciò come una sorta di realtà parallela, ma fortemente collegata e radicata alla realtà quotidiana, poiché sempre più azioni e sempre più rapporti compiuti nello spazio cibernetico hanno conseguenze e ricadute nella vita di tutti i giorni. Le relazioni umane e la circolazione di informazioni trovano nel ciberspazio un terreno fertile che porta a un salto di scala, considerando l'elevatissimo numero di persone raggiungibili.

Lo spazio cibernetico non riconosce alcuna frontiera, non avendo alcun bisogno di un qualsiasi collegamento a un luogo 'fisico': i messaggi e le informazioni vengono scambiati attraverso la rete internet senza che avvenga alcun ritardo od ostacolo dovuto alla distanza tra le due parti comunicanti[21]. Pur essendo innegabile che le infrastrutture tecnologiche, come i *server*, necessarie ad accedere al *cyberspace*, siano effettivamente localizzate all'interno di confini statali e quindi sottoposte alla giurisdizione di un determinato Paese, i flussi di dati vengono scambiati all'interno della rete, senza alcun

[19] ISO/IEC, *Standing Document 6 (SD6): Glossary of IT Security Terminology*, http://www.jtc1sc27.din.de/cmd?level tpl-bereich&menuid 64540&languageid en&cmsare aid=64540 (consultato il 20 giugno 2018).
[20] M.DODGE, R.KITCHIN , *Atlas of cyberspace*, New York, 2002.
[21] D.G.POST, *Governing cyberspace*, in *Wayne Law Review*, 43, 1996, pp.155-171.

possibile collegamento con elementi fisicamente esistenti[22]. Internet permette inoltre relazioni e transazioni tra soggetti che non sanno e non possono sapere l'effettiva locazione geografica della controparte; il luogo in cui avvengono tali incontri è esclusivamente virtuale (si pensi al sito *web* o a una *chat*), indipendente dallo spazio fisico e reale[23]. Pur essendo teoricamente accessibile a chiunque, la libera circolazione nel ciberspazio dipende da numerosi fattori come la disponibilità delle infrastrutture necessarie per il collegamento Internet, la qualità della connessione alla rete e il suo costo. Considerato ciò, si comprende che l'accesso allo spazio cibernetico è più comune nelle aree ricche e industrializzate rispetto a quelle rurali, come risulta raro nei Paesi meno tecnologicamente sviluppati. La fruizione di determinati contenuti è altrettanto dipendente dalla posizione geografica dell'utente e da dove questo concretamente accede al *cyberspace*; alcune pagine *web* si ricaricano offrendo servizi e informazioni collegate a dove si trova il terminale che le consulta. Non va inoltre dimenticato come alcuni Paesi rendano inaccessibili determinati siti e oscurino particolari risultati forniti dai motori di ricerca, giustificando tali mosse con esigenze di tutela dell'ordine pubblico.

La caratteristica principale dello spazio cibernetico, ossia il suo estendersi al di là di confini geopolitici, ha portato a un acceso dibattito sulla sovranità del ciberspazio e su quale soggetto possa legittimamente estendere la propria potestà legislativa e regolamentare nel contesto virtuale

1.2. Il concetto di governance del ciberspazio e la sua evoluzione geo-politica

Occorre specificare che non vi è un'unanimità di vedute nemmeno sul concetto stesso di governabilità di Internet e del mondo cibernetico; il *Working Group on Internet Governance* ne propose una prima definizione[24], ossia lo sviluppo e l'applicazione di principi e valori comuni, così come di norme, regole e schemi decisionali, nel *cyberspace* da parte di governi, di soggetti privati, della 'società civile'. La *governance* dello spazio cibernetico può essere presentata anche come le azioni sia di Paesi che di soggetti privati in tale contesto, al fine di stabilire regole e procedure per attuare politiche pubbliche e

[22] Corte Suprema degli Stati Uniti di America, sentenza *Reno v. American Civil Liberties Union*, 1997, pp.834-835.
[23] D.L.BURK, *Trademarks along the Infobahn: a first look at the emerging law of Cybermarks*, in *University of Richmond Journal of Law and Technology*, 1, 1995, pp.12-14.
[24] Report of the Working Group on Internet Governance, Château de Bossey, giugno 2005, www.wgig.org/docs/WGIGREPORT.pdf (consultato il 12 luglio 2018).

risolvere controversie in un ambito che coinvolge più giurisdizioni[25]. La piena comprensione delle caratteristiche della *governance* cibernetica è un argomento di primaria importanza, poiché comporta il dover regolamentare l'effettività e la legittimità delle pretese statali sul contesto virtuale. La natura transnazionale dello spazio cibernetico mette in seria crisi i concetti tradizionali di sovranità e giurisdizione, spingendo a formulare due distinte domande[26]: può dirsi legittima la richiesta di un Paese di applicare le proprie leggi interne al contesto cibernetico? E come possono essere applicate tali norme nell'ambito delle attività *on-line*?

Il tema della governabilità del *cyberspace* caratterizza il dibattito geo-politico e accademico da diverso tempo; a tal proposito si sono succedute nel corso degli anni diverse posizioni, avanzate sia da studiosi accademici che dai diversi Paesi coinvolti.

Una prima opinione[27] vedeva lo spazio cibernetico come indipendente dalle varie nazioni: la sovranità di Internet e del *cyberspace* doveva essere quindi prerogativa degli utenti e non degli Stati. Si riteneva che il *world wide web* fosse naturalmente portato alla propria autoregolamentazione. Questa era la cosiddetta teoria del *Cyberlibertarianism*[28]. Questa corrente di pensiero trovava il suo fondamento nel fatto che la sfera in cui uno Stato può esercitare la propria potestà legislativa coincide con il territorio delimitato dai propri confini nazionali, mentre le comunicazioni avvenute via Internet oltrepassavano i confini geografici, creando quindi una nuova dimensione delle attività umane. Il voler applicare le norme nazionali in un simile contesto rischiava di diventare una pretesa dalla dubbia legittimità[29].

Un'ulteriore riflessione portava a concludere che voler imporre leggi che non avevano una prospettiva realistica di essere poi effettivamente rispettate avrebbe comportato una perdita di legittimazione per l'intero ordinamento. Le autorità nazionali dovevano rifiutarsi di legiferare in tale materia, anche se avessero avuto la concreta possibilità di farlo; il ciberspazio era visto come ontologicamente indipendente rispetto a ogni Paese[30]. L'avvento della nuova realtà *on-line* andava a minare il collegamento tra il

---

[25] M.MIULLER, J.MATHIASON, L.W.MCKNIGHT, *Making Sense of ' Internet Governance': Defining Principles and Norms in a Policy Context*, Syracuse, 2004, pp.4.
[26] C.REED, *Making laws for cyberspace*, Oxford, 2012, pp.5 ss.
[27] J.P.BARLOW, *A Declaration of the Independence of Cyberspace*, 1996, http://w2.eff.org/Censorship/Intemet_censorship_bills/barlow_0296.declaration (consultato il 20 giugno 2018).
[28] A.MURRAY, *Information technology law: the law and the society*, Oxford, 2010, cap.4.
[29] D.R.JOHNSON, D.POST, *Law and borders-The rise of law in cyberspace*, in *Stanford Law Review*, n.48, 1996, pp.1367-1378.
[30] J.P.BARLOW, *op.cit.*

fenomeno giuridico e la sua localizzazione geografica; veniva meno la legittimazione statale a regolamentare tali fenomeni avvenuti in rete e la possibilità di individuare la normativa applicabile a suddetti accadimenti secondo il luogo dove erano avvenuti[31]. Tale legittimazione trova attualmente il suo fondamento nel consenso prestato dai cittadini nei confronti dell'autorità statale e nel ruolo che essi hanno nel processo legislativo, per esempio attraverso l'elezione di rappresentanti parlamentari. Gli utenti cibernetici non possono però acconsentire ad essere sottoposti a ogni legge di qualsiasi Paese con cui interagiscono nel contesto virtuale, considerato che non hanno alcuna voce in capitolo nella formazione e approvazione di tali norme. Non hanno e non possono avere nemmeno un'effettiva cognizione degli spazi nazionali che stanno attraversando durante la loro navigazione informatica e dei differenti ordinamenti normativi con cui vengono in contatto.

Questo ritratto di entità astratta che provvede alla propria disciplina si è ben presto rivelato però illusorio e fallace. La realtà delle cose ha evidenziato che non è possibile classificare lo spazio cibernetico come dimensione che provvede in maniera autonoma alla propria regolamentazione. Il *cyberspace* è una creazione dell'uomo, e quindi artificiale; non ha una propria natura, né tantomeno una sua intrinseca inclinazione all'autodisciplina.

Le attenzioni dei governi di tutto il mondo si sono concentrate su questo nuovo territorio non appena sono diventati evidenti i benefici che il controllo dello spazio cibernetico poteva portare al proprio Paese. La teoria del *Cyberpaternalism*[32] affermava che non solo era possibile per le leggi nazionali trovare applicazione anche nello spazio cibernetico, ma che questo potesse rivelarsi un approccio utile e vantaggioso. L'idea alla base era che la dimensione virtuale potesse essere regolamentata attraverso una completa conoscenza e un uso consapevole della tecnologia alla base dello stesso *network* di comunicazioni[33]. Internet si stava rapidamente evolvendo da uno spazio sostanzialmente anarchico e indisciplinato a un ambiente effettivamente regolamentabile[34] attraverso continue modifiche alla sua struttura di codici che controlla le modalità e le vie in cui lo spazio cibernetico opera.

---

[31] D.R..JOHNSON, D.POST, *op.cit.*
[32] A.MURRAY, *op.cit.*
[33] J.REIDENBERG, *Lex informatica: the formulation of information policy rules through technology*, in *Texas Law Review*, n.76, 1998, pp.553 ss.
[34] L.LESSIG, *Code 2.0*, New York, 1999, pp.43 ss.

Secondo la corrente di pensiero dominante in questa seconda fase, la dimensione virtuale veniva ora definita come una realtà non diversa e separata da quella fisica e concreta: il mondo *on-line* era pensato come collegato al territorio tradizionale[35] e suo naturale prolungamento. Il ciberspazio era ridotto a nient'altro che una complessa struttura di cavi, fibre e *server*[36]. La possibilità per i singoli Stati di controllare tale struttura, e perciò di legiferare sul mondo virtuale, era collegata all'importanza e alla priorità che i diversi Paesi rivolgevano all'imporre la propria sovranità in tale contesto e ai costi necessari per agire in tal senso. Le autorità nazionali dovevano perciò valutare l'opportunità e la convenienza, sia politica che economica, di imporre la propria potestà sul contesto cibernetico. La sovranità statale sul *web* era vista ora come legittima, considerando inoltre che solo l'autorità nazionale può provvedere alla tutela dei singoli utenti della rete, da parte di pericoli quali virus informatici e *malware*[37]. In questa seconda fase cambiava quindi radicalmente il punto di vista nei confronti dell'intervento diretto degli Stati nel contesto cibernetico; il più grande pericolo per la sopravvivenza del *web* non era più visto nell'eccessiva ingerenza dei Paesi in tale ambito, ma nella loro mancata azione[38].

La terza fase si apriva perciò con la consapevolezza che determinati problemi, come il fenomeno del *cybercrime*, dovessero essere affrontati su una scala globale, attraverso la cooperazione di tutti i soggetti pubblici attivi nel mondo virtuale, sia Stati che Organizzazioni Internazionali. Le controversie in materia di sovranità sul ciberspazio si stavano rapidamente trasformando in dispute tra nazioni e in classici problemi di relazioni internazionali, dove ogni Paese lotta per affermare la propria supremazia e proteggere i propri interessi[39]. Le questioni relative alla *governance* dello spazio cibernetico diventano, da quei momenti in poi, prerogativa delle relazioni tra governi; tali questioni rimangono però prevalentemente irrisolte. Non vi è infatti concordia nell'individuare quali richieste possano essere correttamente avanzate dai vari Paesi e secondo quali modalità possa essere governato lo spazio cibernetico, considerando come manchi un momento costituzionale fondante[40].

[35] J.GOLDSMITH, T.WU, *op.cit.*
[36] J.GOLDSMITH, T.WU, *op.cit.*
[37] K.EICHENSER, *The cyber-law of nations*, in *Georgetown Law Journal*, n.107, 2015, pp.317-380.
[38] J.GOLDSMITH, T.WU, *op.cit.*
[39] K.EICHENSER., *op.cit.*
[40] L.LESSIG, *cit.*

Ancora oggi si contrappongono sostanzialmente due visioni relative alla *governance* del *cyberspace*, che rivelano presupposti ideologici assai diversi tra loro[41]; il blocco occidentale, guidato dagli Stati Uniti, ritiene che gli attuali strumenti giuridici siano efficaci anche nel contesto virtuale e che non ci sia bisogno di ulteriori innovazioni in tale campo. Di diverso avviso sono Paesi come la Russia e la Cina, che sottolineano come la creazione di nuovi strumenti legali di livello internazionale sia ormai inevitabile per governare e garantire la sicurezza dello scambio di informazioni, anche attraverso la rete Internet. Vi è invece unanimità di vedute per quanto riguarda la considerazione dello spazio cibernetico come autonoma dimensione militare. I Paesi occidentali ritengono che il *cyberspace* deve essere considerato un territorio suscettibile di dominazione militare, come i tradizionali domini di terra, aria, acqua e spazio[42]. Concorda con tale visione il governo cinese, che descrive il *cyber warfare* come una vitale quarta dimensione per l'espansione militare, a fianco dei campi di battaglia 'classici' come la terra, i cieli e il mare[43].

Le divergenze sono invece ampie e articolate in merito alle risposte da dare sulla governabilità e gestione dello spazio cibernetico[44]; i Paesi del blocco occidentale, con gli Stati Uniti come capofila, propongono un sistema di *governance* multilaterale, atto a coinvolgere ogni soggetto portatore di interessi relativi al mondo virtuale. I diversi Stati, le organizzazioni non governative, il settore privato, la società civile, gli accademici e i singoli utenti partecipano alla gestione della realtà cibernetica e, più in generale, della rete internet. La Strategia Internazionale degli Stati Uniti per il cyberspace[45], pubblicata nel 2011, impegna il governo statunitense a promuovere tale modello di gestione, e ad adoperarsi per una rete Internet senza restrizioni e censure. L'Unione europea si è espressa con parole simili, auspicando che questo modello di gestione multilaterale del contesto cibernetico possa essere applicato ad ogni livello[46].

---

[41] K.GILES, *Prospects for the rule of cyberspace*, Carlisle PA, 2017, pp.2-3.
[42] Si veda a tal proposito la dichiarazione del Dipartimento della Difesa statunitense, *Department of defense strategy for operating in cyberspace*, 2011, http://www.defense.gov/news/ d20110714cyber.pdf (consultato il 1 agosto 2018).
[43] Ufficio per gli sviluppi militari e di sicurezza della Repubblica Popolare Cinese, http://www.defense.gov/pubs/2013_china report final.pdf (consultato il 1 agosto 2018).
[44] K.EICHENSER, *op.cit.*
[45] *International Strategy for Cyberspace: Prosperity, Security and Openess in a Networked World*, documento di indirizzo rilasciato nel 2011, http:// www.whitehouse.gov/sites/default/files/rss-viewer/international-strategy-for cyberspace.pdf (consultato il 2 agosto 2018).
[46] Risoluzione del Parlamento europeo del 22 novembre 2012 relativa alla prossima conferenza mondiale sulle telecomunicazioni internazionali (WCIT-2012) dell'Unione internazionale delle telecomunicazioni e al possibile ampliamento del campo di applicazione del regolamento delle telecomunicazioni internazionali

La Cina e la Russia, seguiti dagli altri Paesi sotto la loro sfera di influenza politica, ritengono invece che il ciberspazio possa essere governato secondo i dettami tradizionali della sovranità; uno Stato può quindi esprimere il proprio potere nel mondo virtuale e rivendicarne la potestà. Tale visione ha delle conseguenze sia a livello domestico che internazionale; il governo russo, come quello cinese, ha più volte esercitato il proprio potere sul *web* regolando i contenuti che appaiono in rete e sopprimendo e censurando le informazioni che avrebbero potuto causare un rischio per la sicurezza pubblica, *rectius* per la stabilità del governo. Sul versante internazionale, i suddetti Paesi spingono affinché il controllo di Internet passi da una gestione multilaterale, che coinvolge anche i soggetti privati, a forum e riunioni a livello interstatale, come l'Unione Internazionale delle Telecomunicazioni (UIT), al fine di incrementare il potere statale sulla regolamentazione dei contenuti presenti sul *web*. Il primo ministro russo Vladimir Putin annunciò[47] nel 2011 a tal proposito che il proprio Paese si prefiggeva di stabilire il controllo internazionale sul mondo virtuale attraverso la UIT. Una simile proposta accese, come prevedibile, una ferrea opposizione da parte degli Stati Uniti e dell'Unione europea, così come dalla società civile e dalle grandi compagnie di telecomunicazioni[48]. Nell'opinione occidentale, un controllo centralizzato del *web* a livello governativo avrebbe potuto rallentare l'innovazione tecnologica, portando inoltre a una possibile sorveglianza senza precedenti sugli utenti internet, limitandone quindi i diritti fondamentali[49].

Alla Conferenza Mondiale sulle Telecomunicazioni Internazionali del 2012, la Russia propose una revisione del trattato istitutivo dell'UIT secondo il quale ogni Stato avrebbe dovuto avere uguali prerogative e poteri nella gestione dello spazio cibernetico, inclusa l'assegnazione dei domini Internet e il controllo delle infrastrutture necessarie per la connessione[50]. La suddetta proposta venne però bocciata con il voto contrario dei Paesi occidentali; la Russia riuscì infatti solamente a far sì che venisse approvato un protocollo

(2012/2881(RSP)), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52012IP0451 (consultato il 2 agosto 2018).

[47] R.B.MCDOWELL, The U.N. threat to internet freedom, in *Wall Street Journal*, 21 febbraio 2012, https://www.wsj.com/articles/SB10001424052970204792404577229074023195322 (consultato il 3 agosto 2018).

[48] E.PFANNER , *Drafters of Communications Treaty Are Split on Issue of Internet Governance*, in *New York Times*, 6 dicembre 2012, http://www.nytimes.com/2012/12/07/technology/communications-treaty-hungup-on-internet-issue.html (consultato il 3 agosto 2018)

[49] S.Con.Res.50, *A concurrent resolution expressing the sense of Congress regarding actions to preserve and advance the multistakeholder governance model under which the Internet has thrived*, 2012, https://www.congress.gov/bill/112th-congress/senate-concurrent-resolution/50 (consultato il 3 agosto 2018).

[50] Proposta della Russia alla Conferenza Mondiale sulle Telecomunicazioni Internazionali, http://files.wcitleaks.org/public/S12-WCIT12-C-0027!Ri!MSW-E.pdf, (consultato il 3 agosto 2018)

addizionale al trattato che riportava le idee succitate. L'attuale equilibrio geo-politico di poteri nel contesto del ciberspazio si presenta assai instabile, e la situazione si fa sempre più precaria ogni qual volta un nuovo attore, sia un altro Paese o un soggetto privato come una grande compagnia di telecomunicazioni, entra nello scenario sconvolgendo i rapporti di forza preesistenti; non si deve quindi cadere in una semplificazione come ritenere che lo scontro attuale sia tra Paesi occidentali e Stati dell'ex blocco sovietico.

Una simile diversità di vedute testimonia come la governabilità del ciberspazio sia una priorità nel dibattito geo-politico e giuridico globale e come sia una questione ancora irrisolta. La mancanza di un quadro normativo unitario fa sì che manchi una giustiziabilità delle condotte tenute nello spazio *on-line,* creando quindi un possibile *vulnus* all'esercizio dei diritti da parte dei singoli individui in questa nuova dimensione tecnologica. I diritti fondamentali, così come riconosciuti dai Trattati, dalle Convenzioni e dagli standard internazionali, sono infatti validi (o almeno dovrebbero esserlo) anche nello spazio cibernetico; non è però chiaro come tali diritti possano essere esercitati, come siano tutelati e salvaguardati nella nuova dimensione informatica[51]. Ad oggi, il *cyberspace* si presenta come un territorio dai confini potenzialmente illimitati e inesplorati, ma senza un sistema di leggi globalmente accettato, poiché mancano organi dotati del potere normativo e giudiziario, come un cyber-tribunale o un cyber-parlamento, designati a gestire le attività esercitate nello spazio cibernetico e a proteggere i diritti di coloro che vivono tale ambiente.

Un ruolo preminente nella costruzione del mondo *on-line* è stato rivestito dagli Stati Uniti e dall'Unione europea[52]. I primi, forti della loro potenza economica e politica, sono stati la forza dominante nell'espansione della rete Internet, specialmente nei primi anni della sua vita e diffusione nel mondo civile. L'affermazione del *web* come strumento primario di comunicazione ha spinto l'Unione europea a produrre una corposa e variegata normativa in diversi settori rilevanti quali, ad esempio, la proprietà intellettuale, l'*e-commerce,* la protezione e tutela dei dati personali e il rispetto del diritto alla privacy. L'Unione ha ben presente l'importanza fondamentale e strategica della rete internet, ma manca ancora una visuale di insieme che affronti in maniera omnicomprensiva la tematica della governabilità dello spazio cibernetico. L'intervento normativo europeo ha

[51] A.MIHR, *Cyber justice. Human rights and good governance for the internet*, Berlino, 2017, pp.9-10.
[52] Sul perché gli Stati siano gli attori principali nella regolamentazione di Internet e del *cyberspace*, si veda D.DREZNER, *The global governance of the internet: bringing the State back in*, in *Political Science Quarterly*, n.119, 2004, pp 477 e ss.

evidenziato che l'Unione ritiene *l'e-commerce* uno strumento fondamentale per tenere in vita il Mercato Unico, ma ha mostrato anche la consapevolezza di come internet influenzi la vita quotidiana dei singoli individui anche in aspetti non solo prettamente economici. Considerato ciò, sono emersi due punti cruciali attorno i quali ha ruotato (e continua a farlo tutt'ora) il suddetto intervento, ossia il Mercato unico da una parte, e la tutela dei consumatori dall'altra[53]. Il primo aspetto non può essere raggiunto prescindendo da un solo mercato digitale, mentre il secondo rivela la volontà dell'Unione di proteggere la singola persona[54].

1.3. I regimi legali dei territori tradizionali come esempio per la governabilità del ciberspazio

Le posizioni appena esaminate in merito alla governabilità del ciberspazio, portano a diverse conseguenze in merito alle effettive potestà che un singolo Stato può vantare sullo spazio cibernetico.

In base all'idea di sovranità affermata da Cina e Russia, il *cyberspace* può essere assimilato al territorio sovrano di uno Stato; i Paesi dovrebbero quindi assicurare i propri confini e difenderli da attacchi cibernetici. La difesa delle barriere virtuali e informatiche è però ben più complessa rispetto a quella del proprio territorio tradizionale. Il *cyberspace* non ha e non può avere confini; esiste infatti un solo ed unico spazio virtuale su dimensione globale. Un modello di *governance* basato sul concetto di sovranità tradizionale non sembra perciò essere adatto alla realtà cibernetica, considerate le sue caratteristiche ontologiche, e, inoltre, porterebbe a un radicale sconvolgimento dell'attuale *status quo*, per quanto riguarda l'equilibrio geo-politico.

Una concezione opposta a quella che vede il ciberspazio come un naturale prolungamento del territorio fisico di uno Stato è quella che considera il mondo virtuale come bene comune[55], ossia come una risorsa il cui utilizzo non è esclusivo per un singolo utente, ma il cui consumo da parte di una persona riduce la possibilità per gli altri soggetti di usufruirne[56]. Gli Stati Uniti aderiscono convintamente all'idea di ciberspazio come

[53] J.DICKIE, *Consumers and producers in EU E-Commerce Law*, Oxford, 2005, in particolare cap.1 e 7.
[54] A.SAVIN, *op.cit.*
[55] N.GREGORY MANKIW , *Principles of microeconomics*, New York, 2012, pp.224 ss.
[56] G.HARDIN, *The tragedy of commons*, in *Science*, n.162, 1968, pp 1243 ss.

risorsa comune; l'allora Segretario di Stato Hillary Clinton, in un discorso[57] sulla libertà di internet tenutosi nel 2010, fece riferimento al *global networked commons* per definire la rete internet e più specificatamente il *cyberspace*. Coloro che non condividono tale visione sottolineano che le infrastrutture fisiche e le strumentazioni necessarie alla connessione internet, spesso di proprietà di soggetti privati, si trovano nei territori sottoposti a giurisdizione statale, rendendo quindi problematica la concezione del *cyberspace* come risorsa comune[58].

La riflessione sull'effettivo status del mondo cibernetico è necessaria per le similarità che intercorrono tra quest'ultimo e i vecchi domini tradizionali, come l'alto mare, l'Antartide e lo spazio profondo. Questi territori non sono infatti ancora sotto la sovranità di alcun Paese, e il loro caratteristico status non-sovrano è garantito da numerosi trattati internazionali, come si andrà ora ad esaminare. Il contesto cibernetico presenta la stessa peculiare indipendenza, cosicché uno Stato può regolamentare alcuni aspetti del mondo virtuale, ma non può affrontare ogni singola sfida che il governo di tale realtà propone, se non di concerto con gli altri Paesi e gli altri soggetti privati coinvolti nel settore[59].

La rete Internet ha accessi e connessioni in ogni parte del globo, quindi nessun Stato può occuparsi singolarmente della regolamentazione di ogni singolo traffico di dati che intercorre sul *web*.

L'analogia tra *cyberspace* e i territori conosciuti ha ovviamente dei limiti; lo spazio cibernetico, a differenza dell'alto mare, dell'Antartide e dello spazio extra-atmosferico, non è una vera e propria realtà fisica. Inoltre gli strumenti necessari ad accedere al mondo virtuale sono situati all'interno della giurisdizione di singoli Stati; caratteristica peculiare ben diversa da quelle dei domini tradizionali. Nonostante queste differenze, lo spazio cibernetico può essere efficacemente paragonato a questi ultimi, allo scopo di comprendere come governare un territorio che si estende ben al di là dei confini politici di un singolo Paese.

---

[57] H.R.CLINTON, *Remarks on Internet freedom*, 21 gennaio 2010, http://www.state.gov/secretary/20092013clinton/rm/2010/ 01/135519.htm (consultato il 9 agosto 2018)
[58] P.W.FRANZESE, *Sovereignity in cyberspace; can it exist?*, in *Air Force Law Review*, n.1, 2009, pp.17 ss.
[59] K.EINSECHER, *op.cit.*

1.3.1. La potestà governativa dei singoli Stati nell'alto mare

Sin dall'antichità, le popolazioni di ogni parte del globo hanno navigato gli oceani per i più disparati scopi; il mare, nel corso dei secoli, ha visto fiorire ricchi commerci, esploratori alla ricerca di terre lontane e aspre battaglie. Una così lunga tradizione di navigazioni ha portato allo sviluppo di consuetudini, prassi e usi comuni per regolamentare la vita e i rapporti in mare; tali consuetudini furono codificate e sviluppate nel 1958 in un trattato adottato nella prima Conferenza delle Nazioni Unite sul Diritto del Mare[60]. La regolamentazione dell'alto mare[61] fece un ulteriore passo avanti nel 1982, quando venne stipulata la Convenzione delle Nazioni Unite sul Diritto del Mare[62]. L'art.86 della suddetta Convenzione propone una definizione di alto mare negativa, ossia tutte le zone di mare che non rientrano nelle altre aree in cui sono delimitate le acque. L'art.89 afferma inoltre l'indipendenza di tale zona, riconoscendo come nessuno Stato possa validamente sostenere la propria sovranità sull'alto mare. Viene inoltre sancito che tale zona è aperta alle attività di tutti gli Stati, esclusivamente per finalità pacifiche e con adeguato rispetto per gli interessi avanzati dagli altri Paesi nell'esercizio della loro libertà nell'alto mare. Gli Stati hanno inoltre il diritto di far salpare navi battenti la propria bandiera, sulle quali esercitano la propria giurisdizione.

Indipendenza dalla potestà di qualsiasi Stato, libertà di utilizzo delle risorse esclusivamente per fini pacifici e regime di governo stabilito da trattato; sono queste le caratteristiche della *governance* dell'alto mare che possono essere replicate nel contesto dello spazio cibernetico.

1.3.2. Lo spazio profondo e gli altri corpi celesti come territori indipendenti e non sovrani

La corsa allo spazio caratterizzò in maniera profonda il periodo della Guerra Fredda; gli Stati Uniti e l'ex Unione Sovietica ingaggiarono un'accesa competizione per

---

[60] Convenzione internazionale concernente l'alto mare, 13 U.S.T. 2312, 450 U.N.T.S. 11, https://www.admin.ch/opc/it/classified-compilation/19580064/201004140000/0.747.305.12.pdf (consultato il 10 agosto 2018).

[61] Con il termine alto mare si indica l'area di mare posta al di là della Zona Economica Esclusiva, oltre le 200 miglia marine dalla costa e che non è sottoposta alla sovranità di alcuno Stato.

[62] Convenzione delle Nazioni Unite sul Diritto del Mare, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf, consultato il 10 agosto 2018).

essere i primi Paesi a raggiungere lo spazio extra-atmosferico e gli altri corpi celesti, dimostrando così la propria superiorità tecnologica ed economica rispetto alla potenza rivale.

Con il lancio[63] del primo satellite artificiale *Sputnik 1* nel 1957 da parte dell'URSS, lo spazio celeste diventò a tutti gli effetti un dominio territoriale in cui gli Stati potevano aspirare a espandere la propria sfera di influenza; era quindi necessario sviluppare velocemente delle regole di condotta che potessero guidare le azioni dei Paesi in questo nuovo contesto. A tal proposito, nel 1958 l'Assemblea Generale delle Nazioni Unite adottò una Risoluzione[64] in cui l'utilizzo dello spazio celeste veniva limitato a scopi pacifici.

La decisione di considerare il nuovo dominio come indipendente dalle pretese sovrane dei vari Stati fu frutto di accesi dibattiti in sede internazionale. I Paesi del blocco occidentale vedevano infatti una similarità tra le caratteristiche principali dello spazio extra-atmosferico e quelle dell'alto mare, proponendo quindi un simile regime di governabilità[65], mentre l'Unione Sovietica e i suoi alleati ritenevano che vi fossero analogie con lo spazio aereo, sottoposto alla sovranità dello Stato sopra il quale si estende[66]. La posizione sovietica mostrò ben presto un'incongruenza logica, considerando che la rotazione della Terra fa sì che sia in continua mutazione la parte di spazio celeste da sottoporre alla sovranità di un detto Stato, a differenza dello spazio aereo che rimane stazionario sopra un determinato territorio. L'analogia con l'alto mare venne ratificata da una Risoluzione[67] ONU del 1961 che specificava come lo spazio extra-atmosferico fosse libero per l'esplorazione di ogni Stato, ma senza essere soggetto a rivendicazioni nazionali di alcun tipo. Il diritto internazionale proibisce inoltre che i corpi celesti possano essere utilizzati per scopi militari, sancendo ancora maggiormente lo status di indipendenza di questi ultimi.

---

[63] N.DEGRASSE TYSON, *The case for space, why we should keep reaching for the stars*, in *Foreign Affairs*, marzo/aprile 2012, pp.22 e ss.

[64] G.A. Res. 1348 (XIII), U.N. Doc. A/4009, http://www.oosa.unvienna.org/oosalen/SpaceLaw/gares/html/gares13_1348.html (consultato il 13 agosto 2018).

[65] M.J.PETERSON, *The use of analogies in developing outer space law*, in *International Organizations*, n.245, 1997, pp.253-254.

[66] M.J.PETERSON, *ibidem*, pp.254 ss.

[67] G.A. Res. 1721 (XVI), art. A, ¶ 1(b), U.N. Doc. A/5026, http://www.oosa.unvienna.org/oosalen/SpaceLaw/gares/html/gares_16_1721.html (consultato il 13 agosto 2018).

1.3.3. Lo status giuridico dell'Antartide

Sette Stati, tra il 1908 e il 1943, avanzarono numerose pretese territoriali nei confronti di diverse parti del continente antartico[68]. Simili pretese trovarono una loro regolamentazione nel Trattato Antartico[69], firmato nel 1959 da parte delle 12 nazioni che presero parte alle esplorazioni scientifiche del territorio in questione durante l'Anno Geofisico Internazionale (1957-1958). Il Trattato riconobbe agli Stati firmatari il diritto di esplorare liberamente l'Antartide esclusivamente per scopi scientifici e pacifici. Nessuna attività condotta sul continente sarebbe però stata considerata come una base giuridica o politica per rivendicazioni territoriali di alcun tipo, garantendo quindi al territorio antartico uno status di perdurante indipendenza. Viene inoltre proibita alcuna attività militare, in linea con la previsione secondo la quale le attività degli Stati sul continente devono avere esclusivamente finalità pacifiche.

1.4. Nuove modalità di governo per un nuovo territorio come il cyberspace

Nessuno spazio per le rivendicazioni territoriali nazionali, status di non soggezione ad alcuna potestà statale ed utilizzo delle risorse solo ed esclusivamente per scopi pacifici; queste sono le caratteristiche principali delle modalità di governo per i territori ora esaminati, raggiunte attraverso trattati internazionali e forum/assemblee a livello interstatale. Contrariamente a quanto appena visto, non è stata ancora raggiunta una risposta unanime tra i vari soggetti coinvolti, sia pubblici che privati, per quanto riguarda le modalità con cui dovrebbe essere gestito e governato il *cyberspace*. Questa difformità trova la sua ragione anche nel ruolo di primaria importanza che ricoprono le parti private nel contesto cibernetico, a differenza di quanto accade negli altri ambiti come Antartide o spazio celeste. Al fine di individuare un modello di gestione efficiente per il mondo

[68] A.CHANDER, *The new, new property*, in *Texas Law Review*, n.212, 2003, pp.754 e ss. Gli Stati che avanzarono pretese territoriali di vario genere furono l'Argentina, l'Australia, il Cile, la Francia, il Regno Unito, la Nuova Zelanda e la Norvegia. Pur essendo presente un "settore statunitense", gli USA non hanno mai fatto alcuna richiesta ufficiale.

[69] Trattato Antartico, 1 dicembre 1959, https://www.ats.aq/documents/ats/treaty_original.pdf (consultato il 14 agosto 2018). Il numero attuale delle parti firmatarie del Trattato è di 53.

virtuale, occorrerà quindi riflettere approfonditamente su due questioni dirimenti, ossia "chi partecipa alla vita nel *cyberspace?* E chi controlla questa nuova società virtuale?".

1.4.1. Il ruolo dei privati nella governance dello spazio cibernetico: un approccio multilaterale a livello statale o una gestione partecipata "dal basso"?

Come già anticipato nei paragrafi precedenti, vi è un acceso dibattito politico in merito ai metodi più efficaci di gestione del ciberspazio. La Russia, la Cina e i loro alleati sono fautori di un modello di *governance* dello spazio cibernetico basato su un approccio multilaterale a livello statale, dove i vari Stati sono gli unici soggetti dotati di potere decisionale, potendo quindi anche controllare i contenuti diffusi attraverso la rete internet ed eventualmente censurarli. Gli Stati Uniti e gli altri Paesi occidentali supportano invece un modello di *governance* partecipata (*multistakeholder governance*), in cui vengono coinvolti tutti gli attori rilevanti nel contesto virtuale, come i singoli individui, gli accademici e la società civile. La preferenza accordata a una simile gestione del *cyberspace* trova spiegazione nella volontà statunitense di proteggere la libertà di espressione sul *web*, ma anche nella grande influenza che le società di telecomunicazioni hanno nelle scelte del governo USA[70].

Simili opinioni sono però soggette al mutamento degli orientamenti politici in seguito al susseguirsi dei mandati elettorali; l'attuale presidenza statunitense sembra voler esercitare un controllo più incisivo e pressante di quanto avvenuto negli anni precedenti sui contenuti diffusi attraverso il *web.*

Merita una riflessione il fatto che una terza modalità di *governance*, interamente gestita da soggetti privati, sarebbe teoricamente possibile; il ruolo avuto da questi ultimi nello sviluppo e nella diffusione della rete Internet, nonché le prime opinioni, analizzate nei paragrafi precedenti, in merito all'indipendenza del *web* dalle ingerenze statali, lasciano pensare che uno spazio cibernetico privo di influenze del pubblico sarebbe possibile. L'interesse mostrato dagli Stati verso le risorse garantite dal mondo virtuale ha

[70] Le grandi compagnie di telecomunicazioni hanno incrementato sempre più le proprie attività di *lobbying*, atte a influenzare le scelte del governo e del Congresso statunitense. A tal proposito si veda J.BERCOVICI, *Tech Companies Seeking Surveillance Reform Spent $35 Million Lobbying Last Year*, in *Forbes*, 9 dicembre 2013, http:// www.forbes.com/sites/jeffbercovici/2013/12/09/tech-companies-seeking-surveillance-reform-spent-35million-lobbying-last-year/ (consultato il 15 agosto 2018); le cifre complessive spese in attività di *lobbying* dalle società di telecomunicazioni nel 2018 nei soli Stati Uniti sono disponibili al seguente *link https://www.opensecrets.org/lobby/indusclient.php?id=B09*.

però impedito che il modello di *governance* interamente privato venisse poi concretamente attuato, rimanendo quindi niente più che una mera possibilità teorica.

Il diritto internazionale tradizionale vedeva come attori principali i singoli Paesi[71], rendendo l'approccio multilaterale a livello statale nella gestione dei domini tradizionali la scelta preferibile come testimoniato dai trattati internazionali che regolamentano lo spazio celeste e lo status giuridico dell'Antartide. Il ruolo dei soggetti privati nel sistema di sovranità dell'alto mare è comunque rilevante, considerando i traffici che si sono sviluppati via mare nel corso dei secoli e come questi abbiano contribuito a formare un nucleo di norme consuetudinarie (*lex mercatoria*), ma nel XX secolo i principali aspetti relativi al diritto del mare, come le delimitazioni territoriali, furono affrontati a livello governativo e statale, come testimoniato dai numerosi trattati firmati a tal proposito.

La realtà del *cyberspace* fa sì che sia preferibile, per la sua gestione, un modello di *governance* che tenga conto del ruolo e dell'influenza che i soggetti privati hanno avuto e continuano tutt'ora ad avere nella crescita e nello sviluppo del mondo virtuale. Bisogna considerare che le infrastrutture necessarie a una connessione Internet sono infatti spesso di proprietà privata e, senza di esse, lo spazio cibernetico rimarrebbe inaccessibile. Rimarrebbero inoltre inapplicate le politiche decisionali dei governi in merito al contesto informatico, senza la necessaria collaborazione di coloro che possiedono gli strumenti imprescindibili per accedere al *web*. La storia del *cyberspace* evidenzia che gli Stati si sono interessati al nuovo territorio virtuale solo in un secondo momento rispetto ai primi internauti e pionieri del *web*, che hanno contribuito in maniera pressoché esclusiva a gestire il mondo informatico dei primordi, promuovendo una sua autoregolamentazione, secondo i bisogni e le necessità dei vari utenti[72]. Ancora oggi, nonostante il ruolo ormai preponderante dei vari governi nazionali nelle politiche relative al *cyberspace*, soggetti privati[73] di vario tipo mantengono un'importante voce in capitolo nella gestione del contesto cibernetico. Escludere questi ultimi, a favore di una *governance* condotta esclusivamente a livello statale, comporterebbe un aumento dei compiti di regolamentazione per i vari Stati che dovrebbero infatti occuparsi anche delle funzioni

[71] Per una completa analisi dei soggetti di diritto internazionale si rimanda a S.M.CARBONE, *I soggetti e gli attori nella comunità internazionale*, in (a cura di) S.M.CARBONE ET AL., *Istituzioni di Diritto Internazionale*, Torino, 2016, pp.1-47.

[72] Z.BAIRD, *Governing the Internet: Engaging governments, businesses, no-profits,* in *Foreign Affairs*, novembre/dicembre 2002, pp.15 ss.

[73] Si pensi all*'Internet Engineering Task Force* (IETF), un gruppo aperto di ingegneri, informatici, *web designers* e altri esperti del settore informatico, che si occupa di definire e mantenere gli standard per la corretta navigazione nel *web*, o all'*Internet Corporation for Assigned Names e Numbers* (ICANN) che si occupa di distribuire gli indirizzi informatici agli utenti internet.

attualmente svolte dai privati. Non è chiaro se i Paesi coinvolti potrebbero svolgere tali compiti efficacemente. La struttura attuale della rete internet si caratterizza per essere decentralizzata e distribuita, senza un organo centrale di controllo, favorendo quindi una *governance* partecipata e che non sia prerogativa esclusiva dei singoli Stati.

Una particolare occasione di collaborazione tra soggetti pubblici e privati è data dall'*Internet Governance Forum* (IGF); si tratta di una piattaforma di discussione sulla governabilità del ciberspazio progettata dal Segretario Generale delle Nazioni Unite su mandato del *World Summit on Information Society* nel 2006.

In tale ambito gli Stati e gli *stakeholder* privati possono confrontarsi con lo scopo di individuare le corrette modalità di gestione dello spazio cibernetico; pur non avendo alcun mandato imperativo, i risultati dei summit dell'IGF sono certamente tenuti in considerazione dai legislatori statali e internazionali.

A mero titolo di esempio, si ricorda che durante le riunioni dell'IGF sono stati trattati temi importanti e attuali come la *cybersecurity*, le *blockchain* e le criptovalute, le *fake news* etc.

1.4.2. Una struttura di governo per il cyberspace

Dopo aver verificato come la gestione partecipata, che mira a includere anche i soggetti privati nei momenti decisionali, sia la modalità di *governance* preferibile per lo spazio cibernetico, occorre riflettere su quale struttura di governo debba poggiare il mondo virtuale, ossia tramite quali accordi i diversi Stati e i privati possano governare il *cyberspace*.

La prima opzione possibile prevede la mancanza di una struttura di governo, ed è la strada percorsa attualmente; con l'eccezione di trattati per alcune questioni specifiche, come il *cybercrime*[74] o gli standard tecnici per la connessione e la navigazione in Internet, non esistono ad oggi convenzioni internazionali che regolino in maniera omnicomprensiva il mondo cibernetico. La mancanza di specifici accordi a livello interstatale non significa però che non venga applicata alcuna legge; il diritto

[74] Trattato n.185 del Consiglio di Europa, *Convenzione sulla criminalità informatica*, a cui hanno aderito ad oggi 61 Paesi, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016 80081561 (consultato il 21 agosto 2018).

internazionale consuetudinario, ove non trovi spazio la normativa nazionale, regolamenta le nuove fattispecie, incluse le azioni dei singoli Paesi nel contesto cibernetico.

Vi possono essere numerose ragioni alla base della mancanza di un accordo in merito alla *governance* di un determinato territorio[75]. Gli Stati possono infatti non avere le capacità per operare in uno specifico ambito, rendendo quindi superfluo riflettere su come governarlo; era questo il caso dello spazio celeste nel periodo antecedente alle prime esplorazioni avvenute negli anni '50 del secolo scorso. Inoltre, le norme consuetudinarie possono essere così ben sviluppate e comunemente accettate da rendere non necessario un accordo a livello interstatale per trovare una nuova regolamentazione: questo spiega il regime di *governance* dell'alto mare nel periodo antecedente alla stesura di UNCLOS. Un simile accordo può essere sì auspicabile, ma vi possono permanere dubbi e incertezze in merito alle conseguenze per i diversi Stati a seguire delle prime esplorazioni di un territorio completamente inesplorato, che impediscono il concreto raggiungimento di un accordo in tal senso; la complessa situazione giuridico-politica dello spazio celeste negli scorsi anni '60 può essere un esempio paradigmatico in tal senso.

La mancanza di un accordo tra i diversi Paesi coinvolti in merito alle modalità di governo e gestione dello spazio cibernetico trova invece le sue motivazioni nelle diverse opinioni, apparentemente inconciliabili tra loro, a proposito delle metodologie più efficaci per risolvere le problematiche relative alla governabilità del mondo virtuale[76]. L'assenza di una chiara struttura di *governance* porta a una sostanziale instabilità del contesto cibernetico, lasciando spazio a potenziali conflitti tra gli Stati attivi in tale ambito. La mancanza di una *governance* congiunta in ambito cibernetico ha indubbie conseguenze sulla salvaguardia dei diritti considerati dal presente studio. Viene infatti meno un quadro uniforme di tutela, lasciando spazio a una frammentazione normativa che mette a repentaglio la navigazione virtuale dei cibernauti. La possibilità di fruire dei propri diritti dipenderà infatti da fattori quali il luogo di connessione o la nazionalità del *provider*. La crescente importanza, sia sotto l'aspetto politico che economico, del *cyberspace*, nonché le evidenti minacce che possono arrivare da tale 'territorio' (si pensi a fenomeni come il cyberterrorismo o la *cyberwarfare*) stanno conducendo i vari Paesi a concordare sulla

---

[76] D.P.FIEDLER, *Recent developments and revelations concerning cybersecurity and cyberspace: implications for international law*, in *ASIL Insights*, 20 giugno 2012, http://www.asil.org/insights/volume/16/issue/22/recent-developments-and-revelations-concerning-cybersecurity-a (consultato il 22 agosto 2018).

necessità di una regolamentazione completa e uniforme dello spazio cibernetico, considerando inoltre come norme consuetudinarie non si siano ancora sviluppate per tale ambito.

Pur essendo quindi comunemente avvertita la necessità di una nuova struttura di governo per il *cyberspace*, occorre identificare attraverso quali modalità possa essere raggiunto tale risultato.

Una prima opzione potrebbe essere l'utilizzo dello strumento del trattato internazionale, come avvenuto per i domini tradizionali quali l'alto mare, lo spazio celeste e l'Antartide. Una convenzione che affronti ogni tematica relativa al *cyberspace*, una sorta di 'costituzione cibernetica', sembra però ancora lontana dal vedere la luce, per diversi motivi.

In *primis*, le divergenze tra i Paesi occidentali e gli Stati dell'ex blocco sovietico, già affrontate in precedenza, in merito all'approccio con cui affrontare la *governance* dello spazio cibernetico e alle modalità con cui coinvolgere i soggetti privati in tali questioni. Questa differenza di vedute rappresenta un ostacolo rilevante per raggiungere un accordo tra i vari Stati presenti e attivi nel modo virtuale su come regolamentare tale realtà.

Come precedentemente esposto, nel contesto cibernetico non si sono ancora formate norme consuetudinarie tali da poter portare a una loro codificazione in un trattato; non vi è quindi una base normativa condivisa da cui prendere le mosse per formare la nuova "costituzione cibernetica". Bisogna inoltre considerare che, potenzialmente, ogni Stato può avere interessi rilevanti nel mondo virtuale e può agire di conseguenza per difenderli; così tanti interessi contrapposti possono però rallentare significativamente il raggiungimento di una posizione condivisa da ratificare poi in un trattato.

Il contesto cibernetico, a differenza di quanto accaduto per l'Antartide o per lo spazio celeste, coinvolge infatti un numero rilevante di Stati e di attori privati, presentando quindi una realtà ben più complessa e in costante divenire, anche a causa dell'inarrestabile progresso tecnologico del settore. Il Trattato Antartico è stato ratificato solo da 12 Paesi, inclusi i 7 che inizialmente avanzarono pretese territoriali nel nuovo continente.

Appare evidente che ridurre il numero di parti contraenti porta a diminuire il tempo delle contrattazioni e ad aumentare i possibili risultati condivisi[77].

[77] R.HURWITZ, *Depleted trust in the cyber commons*, in *Strategic Studies Quarterly*, Fall 2012, pp.20 e ss.

In conclusione, si può affermare che lo strumento del trattato internazionale non sembra essere adatto a regolamentare una realtà complessa e in continuo divenire come lo spazio cibernetico, dove gli interessi spesso contrapposti degli Stati, nonché il continuo progresso informatico, impediscono il raggiungimento di un punto di vista comune e la stesura di una "costituzione cibernetica" atta a individuare i valori caratteristici del nuovo mondo virtuale.

Un sistema di principi generali può derivare anche dallo sviluppo di norme consuetudinarie e prassi comuni. I soggetti internazionali devono infatti rispettare gli obblighi imposti dal diritto consuetudinario[78], come ricordato dal famoso brocardo latino *consuetudo est servanda*. L'art. 38 dello Statuto[79] della Corte Internazionale di Giustizia elenca la consuetudine tra le fonti del diritto che verranno applicate dai propri giudici nella risoluzione delle controversie, definendola come "*prova di una pratica generale accettata come diritto*".

La formazione del diritto consuetudinario avviene attraverso un processo spontaneo e non formalizzato[80], a differenza di quanto accade per la stesura di un trattato internazionale che richiede l'accordo degli Stati contraenti; la consuetudine, secondo una concezione positivista[81] del diritto internazionale, presenta perciò una forma più sfumata, ma non per questo meno rilevante, della volontà degli Stati rispetto alla fonte pattizia.

Gli elementi fondativi della norma consuetudinaria sono, come noto, essenzialmente due; uno di natura oggettiva o materiale, chiamato *usus* o *diuturnitas*, che indica l'esistenza di una prassi generalizzata e diffusa[82], e uno soggettivo o psicologico, denominato *opinio juris ac necessitatis*, ossia la certezza da parte degli Stati che la prassi di cui sopra trovi fondamento in una specifica norma di diritto o in una data necessità sociale. Il fattore del tempo è un elemento determinante da tenere in considerazione qualora si concepisca la consuetudine come frutto di un processo di formazione spontaneo

---

[78] A.CASSESE, *Diritto internazionale*, Bologna, 2013, pp. 213 ss; T.TREVES, *Diritto internazionale. Problemi fondamentali*, Milano, 2013, pp.222 ss; P.ZICCARDI, voce *Consuetudine (dir.intern.)*, in *Enciclopedia del diritto*, vol. IX, Milano, 1961, pp.486; M.PANEBIANCO, *Diritto internazionale*, Napoli, 2009, pp.160 e ss.

[79] Statute of the International Court of Justice, https://www.icj-cij.org/en/statute (consultato il 26 agosto 2018).

[80] La ricostruzione giuridica che vede la consuetudine come frutto di un processo spontaneo e non formale è comprovata dalla giurisprudenza della Corte Internazionale di Giustizia, in particolare dal caso "Piattaforma Continentale del Mare del Nord". A tal proposito si veda Sentenza della Corte di Giustizia Internazionale, *North sea continental shelf cases*, 20 febbraio 1969, pp.41-43, https://www.icj-cij.org/files/case-related/51/051-19690220-JUD-01-00-EN.pdf (consultato il 27 agosto 2018).

[81] F.SALERNO, *Diritto internazionale. Principi e norme*, Padova, 2011, pp.140 e ss.

[82] A.CASSESE, *op.cit.*

e inconsapevole; è infatti evidente che la creazione di norme consuetudinarie richiede necessariamente il trascorrere di un dato periodo di tempo, che può essere più o meno lungo a seconda di quanto un determinato comportamento è diffuso tra i membri della comunità internazionale

In caso di mancanza di un *corpus* normativo di origine pattizia, il diritto consuetudinario può quindi proporre una struttura regolamentare adatta a governare la vita in un determinato territorio/ambiente; si può ipotizzare il funzionamento di una sorta di clausola Martens[83] anche per il contesto cibernetico. La clausola in questione, redatta in materia di diritto dei conflitti armati, sancisce che, in mancanza di un codice completo applicabile a suddetti conflitti, gli Stati e le popolazioni belligeranti restano sotto la salvaguardia dei principi del diritto delle genti (*ius gentium*), come stabiliti fra le nazioni civili, dalle leggi di umanità e dalle esigenze della coscienza pubblica.

La clausola sembra far riferimento alle norme consuetudinarie, ossia a comportamenti ripetuti nel tempo che, nella convinzione dei vari Paesi, hanno un fondamento giuridico e/o sociale. La consuetudine può quindi svolgere un'importante funzione regolamentatrice in un universo relativamente nuovo ed inesplorato, come quello cibernetico. La risposta data dagli Stati a fenomeni specifici (si pensi al cyber-terrorismo) può funzionare da *best practice* e linea guida a cui attenersi, in caso di simili evenienze, arrivando con il tempo e la prassi a formare una vera e propria base di un diritto consuetudinario cibernetico.

L'opera di rilevazione delle norme consuetudinarie è assai complessa, considerato che possono contribuire alla loro formazione gli interventi diretti degli Stati, attraverso strumenti quali documenti diplomatici, posizioni politiche o dichiarazioni internazionali. Le azioni di Paesi più 'rilevanti' da un punto di vista economico e politico (si pensi agli Stati Uniti, alla Russia o alla Cina) possono perciò influenzare le convinzioni di altri Stati.

La mancata visione comune per quanto riguarda sia lo *status* giuridico dello spazio cibernetico che il ruolo che i privati possono ricoprire nella sua gestione comporta inoltre che difficilmente potrà essere raggiunta in tempi brevi un'opinione condivisa (*opinio juris ac necessitatis*) tra i diversi Stati in merito a una determinata prassi da tenere, impedendo

[83] La clausola Martens è parte integrante del Preambolo della II Convenzione dell'Aja del 1899 sulla guerra condotta per via terra, per poi essere confermata nella IV Convenzione dell'Aja del 1907 sul medesimo tema. La clausola venne poi adottata in altri trattati, come la Convenzione di Ginevra del 1949 e i Protocolli Addizionali del 1977, diventando inoltre base giuridica per numerose pronunce giurisdizionali, come si evince dal parere consultivo emanato dalla Corte Internazionale di Giustizia nel 1996 sulla *Liceità della minaccia e dell'uso delle armi.*

quindi la formazione di una norma consuetudinaria rilevante nel contesto cibernetico. Rimane però la possibilità che la consuetudine emerga anche attraverso la sola azione comune di un ristretto numero di Stati, ovviando in questo modo al problema del mancato conenso che impedisce la stipula di un trattato internazionale.

Lo spazio cibernetico è un contesto in continua evoluzione, spinta da un incessante progresso tecnologico; considerato ciò, si può dedurre che un sistema normativo derivante da un trattato internazionale rischierebbe di diventare ben presto inadatto a regolamentare nuove circostanze ed evenienze, a causa della sua staticità e fissità. La consuetudine si evolve con la pratica da parte dei singoli Stati, dimostrandosi quindi pronta a rispondere all'evoluzione del mondo virtuale e potendo coordinare le azioni dei diversi Paesi coinvolti nello scenario cibernetico, evitando rischi di incomprensioni.

La conclusione della presente analisi evidenzia che l'attuale mancanza di chiarezza e uniformità in merito ai principi basilari atti a regolare le azioni dei soggetti, sia pubblici che privati, coinvolti nel mondo virtuale, non è più sostenibile. Gli Stati devono raggiungere il prima possibile una posizione comune in merito ad alcune definizioni cardine del *cyberspace*, al fine di evitare possibili conflitti che possono originarsi in esso, per poi sfociare nel mondo 'concreto'. Le attuali divergenze in merito alle modalità di governo dello spazio virtuale tra gli Stati più influenti sullo scenario internazionale rendono assai arduo ipotizzare che, entro breve tempo, possa essere stilata una sorta di costituzione cibernetica.

Si può perciò ipotizzare che, allo stato attuale, le modalità più adatte a regolamentare la complessa realtà cibernetica siano trattati internazionali focalizzati su argomenti specifici e settoriali, su cui è perciò più agevole raggiungere un punto di incontro, e lo sviluppo di un sistema di diritto consuetudinario, originato da dichiarazioni e prese di posizione da parte dei singoli Stati a livello multilaterale e/o regionale e dalla costante prassi comune delle parti coinvolte. La natura globale e diffusa dello spazio cibernetico richiederebbe un approccio globale e uniforme che però, per le motivazioni appena esposte, non è attualmente praticabile

1.5. Il controllo militare sullo spazio cibernetico

Un elemento di forte dissidio e contrasto tra le varie potenze rivali nel contesto cibernetico è la militarizzazione del mondo virtuale; tale elemento è strettamente legato al dibattito sulla sovranità sul *cyberspace*, e su come questa debba essere mantenuta. Il

controllo del territorio è infatti un elemento fondamentale affinché uno Stato possa affermare la propria sovranità su di esso, e tale controllo si basa anche sulla difesa militare dei propri confini. La caratteristica principale dello spazio cibernetico è però proprio l'assenza di qualsiasi tipo di barriera; occorre perciò riflettere su quali siano i limiti per l'esercizio della forza militare in un territorio che non è sottoposto alla sovranità, intesa nella modalità derivante da Westfalia, di nessuno Stato e che quindi nessun Paese è obbligato a difendere[84].

Gli esempi forniti dagli altri contesti 'non sovrani', come l'Antartico, l'alto mare e lo spazio celeste, in tema di utilizzo della forza militare sono vari, ma comunque accomunati da una 'militarizzazione' limitata o addirittura inesistente.

Tali limitazioni possono essere la soluzione ideale anche per quanto riguarda il *cyberspace*, considerate le sue caratteristiche.

Innanzitutto nessun Stato, con la tecnologia odierna, può efficacemente difendere i propri confini virtuali[85] e respingere così ogni tipo di attacco informatico. L'incertezza sulle effettive possibilità di ogni singola nazione di controllare militarmente un dato territorio incentivano possibili coordinazioni tra i diversi Paesi coinvolti allo scopo di evitare che un solo Stato prenda il sopravvento militare nel determinato contesto. La suddetta incertezza fa sì che siano attualmente imprevedibili anche le eventuali conseguenze di un attacco cibernetico su larga scala, considerando inoltre che le reti virtuali militari sono strettamente interconnesse con quelle civili[86]; un'arma come un virus informatico può infatti diffondersi senza alcun controllo, non limitandosi a colpire l'obbiettivo prefissato. Una simile interconnessione, a causa della quale un'offensiva militare condotta per via informatica potrebbe avere conseguenze irreparabili, e la sempre maggiore dipendenza di ogni sistema socio-economico dal *web* e dalla connessione internet dissuadono i diversi Stati a ricorrere alle armi cibernetiche. Una progressiva de-militarizzazione del mondo virtuale potrebbe inoltre incentivare gli investimenti in tecnologie informatiche, innescando una spirale virtuosa di cui beneficerebbero sia i soggetti pubblici che privati.

---

[84] K.EICHENSHR, *cit.*

[85] J.S.NYE JR., *Nuclear lessons for cyber security*, in *Strategic Studies Quarterly*, inverno 2011, pp.20 e ss.

[86] S.KANUCK, *Sovereign discourse on cyber conflict under International Law*, in *Texas Law Review*, n.88, 2013, pp.1595-1599; H.H.KOH, *International Law in cyberspace, Remarks as prepared for the delivery to the USCYBERCOM Inter-Agency Legal Conference* (18 settembre 2012), in *Harvard International Law Journal Online*, n.54, pp.1-8.

Nonostante gli aspetti ora citati evidenzino che una limitazione all'uso delle armi nel contesto cibernetico rappresenta la scelta più saggia da intraprendere, le azioni e le politiche adottate dagli Stati non lasciano presagire il raggiungimento di tale risultato in breve tempo. Gli Stati Uniti e il Regno Unito hanno difatti manifestato la loro ferma opposizione al progetto di un trattato internazionale che regolamentasse l'uso degli strumenti informatici durante un conflitto, affermando che l'utilizzo delle armi cibernetiche sarebbe stato disciplinato secondo le esistenti norme di *jus in bello*[87], rifiutando altresì di riconoscere che il *cyberspace* potesse essere teatro esclusivamente di relazioni pacifiche.

Si deve inoltre considerare che diversi Paesi hanno già sviluppato notevoli capacità belliche nel campo della guerra informatica[88]; la de-militarizzazione del contesto cibernetico richiederebbe quindi che detti Stati dismettessero tali armamenti, con quanto ne conseguirebbe in termini di perdita di denaro investito e potere in un campo militare che si annuncia sempre più cruciale nell'imminente futuro. Si comprende perciò come gli Stati siano riluttanti ad abbandonare simili posizioni di forza.

Le minacce militari nello spazio cibernetico possono originare non solo dai vari Paesi, ma anche da soggetti privati come organizzazioni terroristiche; i governi non hanno quindi alcun interesse a procedere a una progressiva de-militarizzazione del *cyberspace*, anche per poter mantenere i propri armamenti ed avere così un'efficace difesa contro simili minacce.

Lo scenario internazionale nel contesto cibernetico, in un mondo così complesso e frammentato come quello virtuale, dove anche le azioni di singole persone possono rappresentare una non trascurabile minaccia per la sicurezza di uno Stato, presenta un numero indefinito e indefinibile di possibili avversari; la funzione deterrente degli armamenti cibernetici ne impedisce quindi una loro completa dismissione.

[87] K.EICHENSHR , *op. cit.*
[88] C.C.DEMCHAK, P.DOMBROSKI, *Rise of a cybered Westphalian age*, in *Strategic Studies Quarterly*, primavera 2011, pp. 32 ss.

1.5.1. Una possibile regolamentazione dell'impiego di forze militari nel contesto cibernetico.

La mancanza di un accordo in merito alla possibile de-militarizzazione del *cyberspace* non comporta che i vari Stati possono agire liberamente, senza limitazione alcuna in termini di armamenti e azioni da compiere.

Una possibile soluzione per ovviare al vuoto normativo è di ritenere applicabile l'esistente diritto dei conflitti armati, applicabile per i terreni di battaglia 'tradizionali', anche al contesto cibernetico. Occorre però chiedersi come tali norme possano applicarsi ad una realtà particolare e complessa come il *cyberspace*[89] e quale possa essere la definizione di 'attacco armato' nella realtà informatica[90].

Una prima esauriente risposta a tali quesiti è stata data da esperti NATO che, riuniti sotto l'egida del Centro di Eccellenza della difesa cooperativa cibernetica del Patto Atlantico, hanno redatto il "Manuale di Tallin sul diritto internazionale applicabile alla guerra cibernetica[91]"

La conclusione fornita dai detti esperti è che l'attuale sistema di *jus ad bellum* e *jus in bello* risulta applicabile anche al contesto virtuale[92] e che occorre valutare le conseguenze di un'azione offensiva condotta nel *cyberspace* per decidere se ha violato il divieto di uso della forza[93]. Viene inoltre riconosciuto il diritto all'autodifesa[94] in seguito a un attacco informatico e che i principi di necessità, proporzionalità e adeguatezza trovano applicazione anche nel mondo virtuale[95].

I conflitti cibernetici sollevano ulteriori dubbi; ad esempio occorre comprendere come possa essere garantita la neutralità di un Paese contro cui non era indirizzato uno

---

[89] W.H.BOOTBY, *Methods and means of cyber warfare*, in *International Law Studies*, n.89, 2013, pp.387 e ss.; J.GOLDSMITH, *How cyber changes the law of war,* in *European Journal of Legal Studies*, n.24, 2013, pp.129 e ss.

[90] Una prima definizione proposta individua l'attacco cibernetico nelle azioni portate avanti con lo scopo di distruggere il sistema informatico nemico per preservare la sicurezza pubblica. A tal proposito si veda O.A.HATHAWAY et al., *The law of cyberattack,* in *California Law Review*, n.100, 2012, pp.817-826; M.C.WAXMAN, *Cyber-attacks and the use of force: back to the futureof article 2(4),* in *Yale Law Journal*, n. 36, 2011,pp.431-36.

[91] Manuale di Tallin sul diritto internazionale applicabile alla guerra cibernetica, Cambridge, 2013.

[92] Regola 20 del Manuale di Tallin: "*Le operazioni cibernetiche eseguite nell'ambito di un conflitto militare sono sottoposte al sistema normativo che regolamenta detto conflitto*".

[93] Regola 45 del Manuale di Tallin: "*Un'operazione cibernetica costituisce aggressione se le sue conseguenze e i suoi effetti sono paragonabili a quelli che si potrebbero conseguire attraverso un'operazione non cibernetica condotta violando il divieto di uso della forza*".

[94] Regola 13 del Manuale di Tallin.

[95] Regola 14 del Manuale di Tallin: *"L'uso della forza da parte di uno Sato nell'esercizio del proprio diritto all'autodifesa deve rispettare i principi di necessità e proporzionalità".*

specifico attacco, considerato che le reti informatiche, sia civili che militari, sono strettamente interconnesse tra loro.

2. Riflessioni conclusive. Autorità, extraterritorialità e giurisdizione nel cyberspace

La riflessione in merito all'effettiva governabilità dello spazio cibernetico ha portato ad individuare nel carattere globale di Internet una delle problematiche principali con cui le tradizionali categorie giuridiche, ideate in un contesto di efficacia chiaramente riconducibile all'interno dei confini nazionali, devono confrontarsi. Al fine di individuare quali sono gli enti incaricati di regolamentare effettivamente il *cyberspace*, occorre primariamente individuare le modalità in cui le norme vengono rispettate nello spazio cibernetico.

Le leggi raggiungono un maggior grado di effettività quando affrontano problematiche che sono ritenute particolarmente importanti dai cittadini che devono sottostare a tali norme. A tal proposito, le autorità legislative devono essere parimenti percepite come vicine da parte dell'intera collettività sociale[96].

La natura diffusa e transnazionale di Internet fa sì che tale sensazione non venga comunemente avvertita dagli utenti cibernetici, che rischiano di dover rispettare leggi e regolamenti di ordinamenti statali avvertiti come lontani e distanti; questo perché le attività *on-line* possono avere potenzialmente effetti in ogni Paese collegato al grande *network* informatico che potrebbe decidere di applicare le proprie norme a dette attività. Considerato ciò, lo spazio cibernetico può teoricamente essere considerato come l'ambiente più regolamentato al mondo[97].

In risposta a questa realtà dei fatti, si è sviluppata la cd. teoria del *cyberlibertarianism* precedentemente analizzata. Questa corrente di pensiero aveva il suo nucleo fondante nel rifiutare che la semplice presenza cibernetica in una diversa giurisdizione statale potesse essere ritenuta sufficiente per applicare le normative di detto Paese[98].

L'opinione che lo spazio cibernetico potesse provvedere a una propria autonoma regolamentazione si è però ben presto rivelata erronea, poiché gli Stati non hanno esitato

[96] S.BIEGEL, *Beyond our control*, Cambridge, 2001, pp.111 ss.
[97] C.MILLARD, *Cyberspace and the no regulation fallacy*, in *Global Telecoms Business Yearbook 1995*, pp.17 ss.
[98] C.REED, *op.cit.*, pp.29 ss.

a far valere le proprie leggi anche nel contesto virtuale, pur essendo questo ontologicamente internazionale e sovranazionale. La regolamentazione delle attività *on-line* non prescinde da una certa valenza extraterritoriale che può però comportare delle conseguenze assolutamente non trascurabili.

La risposta della tradizione giuridico-culturale anglosassone al tema dell'applicazione extraterritoriale della legge nazionale è stata trovata nella cd. *effects doctrine*[99]. Secondo tale teoria, lo Stato ha il potere e la legittimazione a regolamentare le condotte e gli accadimenti che, pur essendo avvenuti al di fuori del proprio territorio nazionale, hanno comunque delle conseguenze e degli effetti all'interno di esso.

Questo potrebbe portare all'aumento di controversie che trovano la loro origine nel fatto che una determinata attività può essere considerata legittima nel Paese in cui viene condotta, ma non in quello in cui ha i suoi effetti; questo perché gli standard normativi degli Stati coinvolti sono radicalmente diversi. In tali circostanze, l'applicazione extraterritoriale della normativa statale può inviare il messaggio che la legge dell'altro Stato viene considerata inferiore e non degna di rispetto[100], con le conseguenze che questo può avere nei confronti dei cittadini che a tale legge sono sottoposti.

L'Unione europea ha risposto alle problematiche appena menzionate attraverso l'utilizzo di specifici strumenti di diritto internazional-privatistico volti ad eliminare, o perlomeno ridurre al minimo, eventuali controversie su quali leggi applicare al contesto delle attività cibernetiche.

Per quanto riguarda la regolamentazione delle obbligazioni di natura extra-contrattuale, si deve far riferimento a quanto previsto dal Regolamento (CE) 864/2007, comunemente noto come Roma II[101]. La regola generale individua il criterio di collegamento nel luogo in cui si verifica il danno, indipendentemente da quello in cui è avvenuto il fatto che ha causato il danno stesso. Limitando l'analisi all'ambito di indagine del presente studio, ossia i diritti fondamentali, l'art. 1 (2) (g) esclude la violazione dei diritti della personalità dall'applicazione del Regolamento Roma II. Questa esclusione è data dal mancato accordo tra i Paesi membri in merito alla legge alla quale si dovrebbe

[99] Per una completa analisi della *effects doctrine* si rimanda a A.PARRISH, *The effects test: extraterritoriality's fifth business*, in *Vanderbilt Law Review*, n.61, 2008, pp.1455 ss.
[100] C.REED, *op.cit.*
[101] Regolamento (CE) n. 864/2007 del Parlamento europeo e del Consiglio, dell'11 luglio 2007, sulla legge applicabile alle obbligazioni extracontrattuali (Roma II) in GUUE L 199, 31 luglio 2007, pp.40-49.

far riferimento per la responsabilità civile per il danneggiamento dei diritti relativi alla persona.

In mancanza di una norma di conflitto uniforme a livello europeo sancita dal Regolamento Roma II, attualmente la legge applicabile ai casi di violazione di diritti della personalità attraverso Internet deve essere individuata attraverso norme di conflitto individuate su base nazionale per ogni Stato membro[102]. Questa difformità può avere degli effetti collaterali da non trascurare, come una mancanza di prevedibilità della legge e un aumento delle controversie, con un conseguente aumento dei costi per i soggetti coinvolti.

L'elaborazione di una norma di conflitto applicabile a livello europeo deve tenere in conto specifici valori, quali la lotta al fenomeno del *forum shopping*, la ricerca di una certezza del diritto applicabile facendo riferimento a specifici elementi di collegamento, il favore per la libera circolazione di persone e capitali attraverso il territorio dell'Unione europea come prefissato dai Trattati istitutivi[103]. Al momento basti evidenziare come il carattere transnazionale dello spazio cibernetico ponga a dura prova le tradizionali categorie giuridiche, imponendo l'individuazione di nuove modalità di tutela per i diritti fondamentali interessati dalle attività informatiche.

Il carattere ubiquo e transnazionale della rete informatica comporta delle problematiche anche in tema di giurisdizione, *rectius* nell'individuare quale giudice deve ritenersi competente a giudicare in materia di illeciti nati nel *cyberspace* e quindi con una dimensione potenzialmente globale. Nel caso di violazione di diritti della personalità attraverso mezzi informatici, si pensi a tal proposito alla pubblicazione su Internet di contenuti potenzialmente diffamatori e infamanti, la Corte di giustizia dell'Unione europea ha stabilito che[104] il ricorrente può decidere se agire dinanzi alla ai giudici del Paese in cui il soggetto che ha diffuso gli articoli controversi ha il proprio stabilimento o davanti alle corti nazionali dello Stato in cui ha il proprio centro di interessi e questo per la totalità del danno. Rimane altrimenti la possibilità di azionare singoli procedimenti nei diversi Paesi per la parzialità del danno lamentato in ogni singolo Stato. Questa soluzione non deve essere interpretata come una sorta di ripensamento sul criterio del *locus damni*,

[102] J.GARRASCOSA GONZALÈZ, *The Internet – Privacy and rights relating to personality*, Londra, 2015, pp.391 ss.
[103] J. GARRASCOSA GONZALÉZ, *ibidem.*
[104] Corte di giustizia dell'Unione europea, sentenza del 25 ottobre 2011, *eDate*, cause riunite C-509/09 e C-161/10, ECLI:EU:C:2011:685.

ma piuttosto come un suo adattamento alle esigenze di un mezzo di comunicazione dagli effetti potenzialmente globali come la rete Internet[105].

Il dilemma dell'extraterritorialità spinge il legislatore nazionale a chiedersi dove e con quali modalità può acquisire l'autorità necessaria per far sì che le norme emanate vengano rispettate anche da soggetti che non si trovano all'interno della propria giurisdizione, così come spesso accade nel contesto cibernetico, considerati gli utenti che si connettono quotidianamente da ogni parte del globo.

Assumendo il punto di vista degli individui tenuti a rispettare le leggi, si comprende che un legislatore ha tanta autorità quanto le persone si sentono in obbligo di dover rispettare tali norme; non è una questione di regole imposte, ma di volontà interna del singolo soggetto di sottostare alle regole[106]. Possono sussistere diversi motivi che portano gli utenti cibernetici a non avvertire tale volontà[107].

In primis, la mera applicabilità di una norma non comporta di conseguenza la sua giustiziabilità; in mancanza di un adeguato meccanismo volto a far sì che la legge in questione venga rispettata, l'internauta non dovrà temere alcunché nel caso in cui decida di violarla. L'utente virtuale può inoltre trovarsi nell'impossibilità di rispettare una specifica norma emanata da un legislatore nazionale poiché è in aperta contraddizione con quella di un altro ordinamento. Questo accade perché la regolamentazione dello spazio cibernetico non ha ancora assunto quel carattere unitario e uniforme immune alle differenze dei singoli sistemi nazionali. Un'ulteriore motivazione può essere data dal fatto che l'internauta può essere all'oscuro che una specifica norma di un Paese diverso dal suo vieta il comportamento che sta attualmente tenendo in Internet: non si può logicamente pretendere che ogni persona sia a conoscenza di ogni specifica norma emanata in ogni Paese.

La mancanza di una disciplina chiara e uniforme in merito allo spazio cibernetico è data anche dalle divergenze in merito a cosa effettivamente sia il *cyberspace*. Lo studio fin qui condotto ha posto in evidenza come vi siano diverse correnti di pensiero in merito alla questione, caratterizzate anche dai diversi interessi delle parti coinvolte. Ad una visione del mondo virtuale come ambiente in cui anche i soggetti privati hanno voce in capitolo, propugnata dagli Stati Uniti e dai Paesi cd. occidentali, si contrappone una

[105] S.M.CARBONE, C.E.TUO, *Il nuovo spazio giudiziario europeo in materia civile e commerciale*, Torino, 2016, pp.142 ss.
[106] H.L.A. HART, *The concept of law*, Oxford, 1994, pp.89-91.
[107] C.REED, *op.cit.*, pp.73 ss.

corrente di pensiero sostenuta da nazioni quali la Russia e la Cina che vedono lo spazio cibernetico come estensione della realtà fisica, dove solamente gli Stati possono esercitare una qualche potestà legislativa e regolamentatrice.

Il dilemma principale da risolvere per individuare le effettive modalità di gestione del *cyberspace* è proprio quello relativo alla sua natura. Prima di poter pensare a come governare un determinato ambiente, bisogna capirne le sue caratteristiche costitutive.

A parere di chi scrive, lo spazio cibernetico non può essere disciplinato con l'utilizzo dei tradizionali strumenti giuridici data la sua realtà ontologica; si tratta infatti di una realtà che i privati hanno contribuito, e stanno ancora contribuendo, a plasmare e influenzare in maniera importante. Le azioni di grandi società industriali come Google, Facebook e Apple hanno un peso non trascurabile nella formazione delle *policies* da rispettare nel mondo informatico: i legislatori, sia nazionali che sovranazionali, devono quindi tenere conto anche dell'influenza che hanno soggetti privati nella formulazione di norme e disposizioni che trovano attuazione nel *cyberspace*.

Si sta inoltre discutendo di una realtà in continuo mutamento, soggetta all'incessante evoluzione tecnologica: è arduo prevedere come lo spazio cibernetico cambierà nell'immediato futuro ed è quindi ancora più complesso individuare norme e regolamenti che possano avere una qualche valenza duratura.

Alla luce di quanto esposto, si conferma quanto anticipato all'inizio della trattazione: far riferimento alla tutela dei diritti fondamentali può essere il primo passo necessario da cui partire per regolamentare il nuovo mondo virtuale. In mancanza di ulteriori elementi di accordo, la salvaguardia di determinati valori e principi può rappresentare la base da cui far partire un dialogo politico e giuridico costruttivo tra i diversi soggetti coinvolti, sia pubblici che privati, e che possa risentire solo minimamente del progresso tecnologico.

Capitolo 2

Una riflessione sul carattere fondamentale del diritto all'accesso a Internet e sulla connessione al ciberspazio tra libera espressione e intervento statale

Sommario: Introduzione – 1. Il diritto di accesso a Internet è un nuovo diritto fondamentale? – 1.1. Motivazioni a sostegno del carattere fondamentale del diritto all'accesso a Internet. – 1.2. Ragioni contrarie al riconoscimento del diritto all'accesso a Internet come nuovo diritto fondamentale. - 1.3. Il diritto all'accesso a Internet può

essere considerata una nuova norma consuetudinaria? - 1.4. Riflessioni sulle possibili conseguenze dell'affermazione del diritto a Internet come fondamentale. - 2. La connessione a Internet come strumento per la realizzazione del diritto alla libera espressione nell'epoca digitale. – 2.1. Il rapporto tra l'accesso a Internet e altri diritti fondamentali. – 3. Il libero accesso a Internet come diritto sociale. – 3.1. La responsabilità degli Stati nel raggiungimento dell'obbiettivo della connettività universale. - 4. Il diritto all'accesso a Internet nell'ordinamento Ue: diritto fondamentale o servizio universale? – 4.1. La connessione al world wide web e la sua possibile regolamentazione come "servizio universale" secondo quanto affermato dalla direttiva 2002/22/CE. - 5. Il diritto all'accesso a Internet e le esperienze politiche nazionali, con una particolare attenzione al caso italiano - 6. Un diritto all'accesso ad una rete Internet neutrale. Il diritto all'uguaglianza cibernetica e la net neutrality. – 6.1. Il diritto all'accesso a Internet e la net neutrality nel Regolamento (UE) 2015/212. – 6.2. La net neutrality nell'esperienza statunitense. - 6.2.1. La qualificazione degli Internet Service Provider come common carriers. - 7. Riflessioni conclusive

Introduzione

Internet ha radicalmente influenzato l'epoca moderna, conducendo di fatto l'umanità nella società digitale. Le nuove tecnologie sono ormai strumenti imprescindibili per l'essere umano per le più piccole e comuni esigenze della vita quotidiana, così come per la partecipazione alla vita politica e sociale della propria comunità.

Il collegamento tra democrazia e informazione è sempre stato chiaro all'uomo, sin dall'antichità. Aristotele affermava infatti che l'ordine democratico può essere stabile e duraturo esclusivamente in un contesto di libertà, dove tale libertà viene garantita dall'informazione[108]. Il progresso tecnologico permette attualmente ai cittadini di poter accedere in maniera precisa e tempestiva alle notizie, in maniera tale da poter svolgere con cognizione di causa un ruolo all'interno della propria *polis*[109]. Attraverso una corretta informazione, il singolo individuo dovrebbe essere in grado di rimanere al corrente delle attività e delle decisioni degli amministratori della *res publica*.

[108] ARISTOTELE, *La Politica*, in (a cura di) C.A.VIANO, *Politica e Costituzione di Atene di Aristotele*, Torino, 1992, pp.273-274.

[109] P.E.ROZO SORDINI, *La libertà di espressione nell'era digitale: disciplina internazionale e problematiche*, ISPI Working Paper n.52, Ottobre 2013, https://www.ispionline.it/sites/default/files/pubblicazioni/wp_52_2013.pdf (consultato l'11 aprile 2019).

Lo Stato, per poter assicurare un'effettiva trasparenza nella gestione degli affari pubblici, non può però limitarsi a rendere disponibili le informazioni a tal proposito, ma deve altresì impegnarsi nel farle circolare rendendole liberamente accessibili ai propri cittadini. Internet può essere quindi un valido strumento per l'affermazione del governo democratico poiché ne garantisce la base fondamentale: la libertà di espressione.

Non si deve però pensare che la rete informatica svolga esclusivamente una funzione comunicativa; lo spazio cibernetico è una dimensione dove le persone possono comprare beni o servizi, studiare, entrare in contatto con la Pubblica Amministrazione, lavorare e stringere rapporti di ogni tipo[110]. Il confine tra dimensione reale e virtuale si fa sempre più labile, poiché le azioni intraprese nel *cyberspace* hanno importanti conseguenze anche nella realtà concreta. La piena realizzazione dell'individuo nell'epoca moderna non può quindi prescindere dall'utilizzo dei mezzi informatici; questo concetto può essere riassunto efficacemente in *digito ergo sum*[111], ossia esisto compiutamente solo e in quanto presente nella dimensione cibernetica.

L'importanza di avere a disposizione una connessione al *cyberspace* è perciò innegabile nella società moderna; considerato ciò, è possibile definire il diritto all'accesso a Internet come un nuovo valore fondamentale?

La risposta a questa domanda non può prescindere da un attento studio delle caratteristiche di tale diritto, che può essere declinato secondo due aspetti apparentemente contrapposti. Da una parte libertà individuale di utilizzare gli strumenti tecnologici per essere informati, dall'altra pretesa di una prestazione da parte dello Stato affinché rimuova gli ostacoli all'accesso allo spazio virtuale per i cittadini, garantendo inoltre loro una connessione effettiva e stabile.

In altre parole, l'accesso a internet può essere considerato come diritto fondamentale a sé stante, come elemento strumentale e accessorio alla realizzazione di ulteriori valori come la libertà di espressione o ancora come diritto sociale?

Risolvere questo quesito non è un mero esercizio teorico, poiché il ruolo dello Stato nel garantire una connessione informatica per i propri cittadini cambia radicalmente a seconda della concezione che si ritiene debba avere il diritto all'accesso a Internet.

---

[110] G.D'IPPOLITO, *L'accesso a Internet come diritto sociale. Ecco perché è necessario,* in *Agenda Digitale*, 29 marzo 2017,https://www.agendadigitale.eu/infrastrutture/occorre-una-prospettiva-umana-per-la-nuova-generazione-di-internet/ (consultato l'11 aprile 2019).

[111] T.E.FROSINI, *Il diritto costituzionale di accesso a Internet,* in *Rivista Telematica Giuridica dell'Associazione Italiana dei Costituzionalisti*, n.1/2011, pp.1-17.

Il primo passo da compiere è aprire una riflessione sulle caratteristiche tecniche e sul contenuto concreto che questo diritto deve avere, per capire poi quali sono le necessarie azioni politiche e normative a riguardo. L'ambiente cibernetico vede la coesistenza di diverse categorie di soggetti, dallo Stato al semplice utente individuale passando per le grandi compagnie informatiche: la realizzazione del diritto all'accesso a Internet deve giocoforza passare dalla collaborazione di questi attori. Il primo obbiettivo raggiungibile dal potere pubblico è la riduzione del cd. *digital divide,* intendendo con tale terminologia il *gap* che intercorre tra chi ha la possibilità di accedere alla rete Internet e chi, per motivi sociali, politici e/o economici ne è invece escluso. Le azioni per ridurre questo divario sono molteplici, come garantire alla totalità di cittadini la possibilità di fruire di una connessione Internet alle migliori condizioni tecniche possibili. Prendendo ad esempio la realtà italiana, non vi è nessun obbligo per le compagnie di telecomunicazioni di rendere disponibile la banda larga per l'accesso a Internet a ogni nucleo famigliare/abitazione, così come invece succede per la linea telefonica. Un intervento simile comporterebbe certamente un cospicuo esborso economico, finanziabile attraverso un fondo comune tra i vari operatori che viene ora utilizzato per garantire la rete di telefonia. Un ulteriore passo da compiere andrebbe nel verso di incentivare l'alfabetizzazione digitale dei cittadini attraverso percorsi scolastici *ad hoc*. Per poter usufruire delle potenzialità di Internet, le persone devono prima essere messe in grado di comprenderle e capirle appieno.

La prima parte del capitolo vuole rispondere alla domanda se tale diritto possa essere considerato come fondamentale, proponendo sia argomenti a sostegno di tale tesi che motivazioni di segno opposto. La riflessione si sposta successivamente sul ruolo che le nuove tecnologie hanno nell'attuazione del diritto alla libera espressione e alla libera manifestazione del pensiero, per osservare come tali principi trovino spazio in un contesto digitale. Come precedentemente accennato, Internet non è più solamente un mezzo di comunicazione, ma anche uno strumento per la piena realizzazione sociale del cittadino all'interno della propria comunità; la terza parte dell'analisi è quindi incentrata sulla possibile concezione del diritto all'accesso a Internet come diritto sociale e sul ruolo degli Stati nel garantire la connessione al *web* per i propri cittadini. L'attenzione viene poi rivolta al quadro normativo europeo e italiano a tutela di uno spazio cibernetico libero e accessibile, per riflettere su quali strumenti legislativi sono stati effettivamente utilizzati e a quale scopo. A conclusione dell'indagine occorre riflettere su quale Internet sia necessaria nell'epoca attuale e quali caratteristiche debba avere per poter funzionare come

strumento per la realizzazione di altri diritti. Alcuni contenuti e servizi presenti in rete devono essere privilegiati rispetto ad altri? O è preferibile un *web* neutrale e paritario?

1. Il diritto di accesso a Internet è un nuovo diritto fondamentale?

4 persone su 5 ritengono che avere a disposizione una connessione a Internet debba essere considerato un diritto fondamentale per l'essere umano: questo è il risultato di un sondaggio commissionato dalla rete televisiva britannica BBC nel 2010 che ha coinvolto più di 27mila persone in 26 diversi Paesi[112]. L'opinione comune sembra ritenere l'accesso al *world wide web* come un'esigenza imprescindibile per l'epoca attuale. Occorre poi ricordare che il sondaggio ha avuto luogo ben 10 anni fa, in un'epoca in cui il web 2.0 stava muovendo i primi passi. La rapida diffusione dei *social network* avvenuta perlopiù successivamente (l'applicazione di Instagram è stata infatti lanciata sul mercato proprio nel 2010) ha certamente influenzato la percezione relativa alla necessarietà di una connessione Internet per le esigenze della vita quotidiana. Storicamente un determinato diritto si afferma come fondamentale quando l'insieme dei consociati ne avverte la profonda necessità; è il popolo a definire come essenziale uno specifico valore e a reclamarne l'attuazione[113].

Non vi è dubbio alcuno sul fatto che la rete Internet ha assunto un ruolo importante nella società moderna, diventandone un elemento discriminante: chi può accedere alla dimensione cibernetica gode di poteri e opportunità che sono di fatto preclusi a coloro che non hanno a disposizione le strumentazioni adatte alla navigazione in rete. L'utilizzo delle nuove tecnologie ha dato vita all'era dell'accesso[114]. Oggetto del sinallagma contrattuale non è più la proprietà di un bene, ma la possibilità di poterne usufruire: di "accedervi" per l'appunto. Non è necessario che questo comporti il passaggio di proprietà del bene oggetto di trattativa. Si pensi alle piattaforme di *streaming* come Youtube, dove si può avere accesso a una selezione pressochè infinita di contenuti multimediali senza dover acquistarne la proprietà e mantenendo quindi intatta e disponibile per altri soggetti la risorsa interessata. Il contenuto in questione, che sia una foto, una canzone o un video, non viene consumato ed esaurito dall'interazione con uno o più soggetti, ma rimane

[112] I risultati del sondaggio sono disponibili al seguente link http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf (consultato il 20 febbraio 2019).
[113] N.BOBBIO, *L'età dei diritti,* 1990, Torino, pp.12-15.
[114] J.RIFKIN, *L'era dell'accesso. La rivoluzione della New Economy,* Milano, 2000.

disponibile per una platea di consumatori potenzialmente indefinita. L'utente può acquistare la possibilità di ascoltare una canzone senza diventare proprietario della traccia musicale o di vedere un film senza effettivamente avere a disposizione la pellicola corrispondente. Nell'era dell'accesso, la differenza non viene data dalla proprietà dei mezzi di produzione, ma dall'avere a disposizione la tecnologia necessaria per accedere alla dimensione cibernetica. Circa il 55 % della popolazione mondiale non ha attualmente tale disponibilità[115]; occorre perciò chiedersi se la connessione al *world wide web* è un privilegio riservato esclusivamente alle popolazioni che risiedono nei Paesi industrializzati o è invece un diritto che deve essere tutelato e riconosciuto su scala globale.

In altri termini, il diritto a una connessione Internet può essere considerato come un nuovo diritto fondamentale?

1.1. Motivazioni a sostegno del carattere fondamentale del diritto all'accesso a Internet

Il concetto di diritto fondamentale è mutato nel corso del tempo[116] seguendo le esigenze e le necessità di una società in continua evoluzione[117]dall'epoca dell'approvazione della Dichiarazione Universale dei Diritti Umani[118]. Il progresso tecnologico può condurre a situazioni tali da suscitare l'esigenza tra i consociati di nuovi principi e valori, come il diritto alla privacy genetica, all'identità informatica o, per l'appunto, all'accesso a internet[119].

La natura unica dello spazio cibernetico ne fa un mezzo di comunicazione totalmente diverso da tutti gli altri *media*: la sua capacità di far circolare le informazioni in tempo reale permette infatti di aprire nuove frontiere per la libertà di espressione, dando modo a ogni utente di avere una reale cognizione di causa sui fatti su cui si esprime[120].

---

[115] The State of Broadband 2018: Broadband catalyzing sustainable development, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.19-2018-PDF-E.pdf (consultato il 14 aprile 2019).

[116] P.DE HERT, D.KLOZA, *Internet (access) as a new fundamental right. Inflating the current rights framework?,* in *European Journal of Law and Technology*, vol.3,n.3, 2012, pp.1-32.

[117]M.ODELLO, S.CAVANDOLI, *Emerging areas of human rights in the 21st century*, Londra, 2011, pp.13 ss.

[118] Assemblea Generale delle Nazioni Unite, Dichiarazione dei Diritti Umani, 10 dicembre 1948, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/itn.pdf (consultato il 21 febbraio 2019).

[119] R.BROWNSWORD, M.GOODWIN , *Law and the technologies of the twenty-first century*, Cambridge, 2012, pp.225-245.

[120] I.DE SOLA POOL, *Technologies of freedom*, Boston, 1984, pp.30 e ss.

Internet consente inoltre altre funzioni sociali che sono precluse ai media tradizionali: permette infatti al singolo utente di condividere le proprie idee su scala globale senza dover ricorrere a intermediari. Il singolo individuo non è più mero fruitore di notizie, come accade ancora oggi con la carta stampata e la televisione, ma diventa egli stesso creatore di contenuti. Il Parlamento europeo ha recentemente segnalato che il *cyberspace* è diventato lo spazio principale dove dissidenti politici, intellettuali, attivisti per i diritti umani e semplici cittadini possono far sentire la propria voce[121]. Internet permette di ribaltare il tradizionale paradigma dell'informazione, rendendo l'utente finale non solo un passivo recettore di notizie e dati, ma anche un soggetto attivo che rielabora a sua volta tali informazioni e le condivide sul *web*[122]. Lo spazio cibernetico è inoltre il luogo dove è possibile recuperare contenuti in tempo reale a un prezzo irrisorio, se non addirittura nullo; la diffusione del sapere non è mai stata così agevole come nell'era cibernetica. Internet è inoltre uno strumento attraverso il quale si creano nuovi canali di comunicazione tra la cittadinanza e l'apparato politico-istituzionale dello Stato. La Pubblica Amministrazione dialoga con i cittadini avvalendosi di strumenti informatici. Le peculiarità specifiche di Internet rendono evidente come si sia sentita la necessità di discutere di un diritto all'accesso al *web* e non ai media tradizionali come giornali e televisione

Considerato ciò, è opinione comune[123] che nessun provvedimento dovrebbe limitare l'accesso alla rete internet nel pieno rispetto di quanto previsto dalla Dichiarazione Universale dei Diritti Umani. Lo *Special Rapporteur* delle Nazioni Unite Frank La Rue ha suggerito che le limitazioni ai contenuti accessibili attraverso lo spazio cibernetico devono essere quanto più circoscritte possibili, auspicando invece che una connessione al *web* sia resa alla portata di tutti i cittadini attraverso specifiche politiche pubbliche[124].

---

[121] Parlamento europeo, Risoluzione P6_TA(2006)0324 sulla Libertà di espressione su internet, 6 luglio 2006, https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2006-0324+0+DOC+XML+V0//EN (consultato il 21 febbraio 2019).

[122] Consiglio delle Nazioni Unite sui Diritti Umani, Risoluzione A/HRC/20/L.13 sulla promozione, protezione e godimento dei diritti umani su internet, 29 giugno 2012, par.3, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement (consultato il 25 febbraio 2019).

[123] A.MURRAY, *A Bill of Rights for the Internet*, 2010, *http://theitlawyer.blogspot.com/2010/10/bill-of-rights-for-internet.html*, (consultato il 25 febbraio 2019).

[124] Consiglio delle Nazioni Unite sui Diritti Umani, *Report dello Special Rapporteur sulla promozione e protezione del diritto alla libera espressione e opinione, Frank La Rue*, A/HRC/17/27, 6 maggio 2011, https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (consultato il 25 febbraio 2019).

Riconoscere il carattere di diritto fondamentale all'accesso a Internet è una risposta ai tentativi di limitare la libertà dello spazio cibernetico attraverso gli strumenti della censura e del controllo governativo[125]. Il successo della rete informatica è intrinsecamente connesso alla sua struttura distribuita e aperta[126], progettata senza dover tener conto di confini politici o geografici[127].

Nonostante ciò, nel corso degli ultimi anni gli utenti cibernetici hanno dovuto fare i conti con alcuni confini "tecnici" che hanno progressivamente ostacolato la libera circolazione delle informazioni[128].

Secondo quanto osservato da La Rue, tali restrizioni arbitrarie possono assumere numerose forme, come la criminalizzazione della libertà di espressione, gli attacchi cibernetici, la disconnessione degli utenti "sgraditi", un'inadeguata protezione della privacy e dei dati personali e l'imposizione di oneri normativi ed economici insostenibili agli intermediari informatici come i gestori dei motori di ricerca. L'evoluzione tecnologica di Internet sembra inoltre portare a dotare il *web* di funzionalità e strumenti che ne permettono un più agevole controllo. Sergey Brin, co-fondatore di Google, ha affermato che le minacce alla libertà del *cyberspace* non derivano solamente dalle censure apportate dagli Stati, ma anche dalle azioni dell'industria dell'intrattenimento e delle telecomunicazioni che mettono a repentaglio la privacy dei loro clienti e dall'atteggiamento di grandi compagnie come Apple o Facebook che adottano politiche assai restrittive nel decidere quali *software* accettare sulle proprie piattaforme[129].

La progressiva tendenza verso tali atteggiamenti di controllo e censura ha come risposta un'aumentata attenzione verso la tutela dei diritti umani. La richiesta per un *cyberspace* libero può accendere l'attenzione politica su quanti individui nel mondo non hanno ancora accesso alla rete internet per motivi economici o culturali. La formulazione di uno specifico diritto alla connessione *web* può aiutare a combattere il fenomeno del *digital divide*, ossia il divario tra chi ha, o perlomeno può permettersi di navigare in rete, e chi invece non ne ha gli strumenti. Al fine di diminuire tale divario, si deve agire su due

---

[125] P.DE HERT, D.KLOZA, *op.cit.*
[126] J.BING, *Building cyberspace:a brief history of Internet*, in (a cura di) L.A.BYGRAVE, J.BING, *Internet governance. Infrastructure and institutions*, Oxford, 2009, pp. 230 ss.
[127] L.GUERNSEY , *Welcome to the World Wide Web. Passport, please?*, in *The New York Times*, 15 marzo 2001, https://www.nytimes.com/2001/03/15/technology/welcome-to-the-world-wide-web-passport-please.html (consultato il 20 febbraio 2019).
[128] J.GOLDSMITH, T.WU , *Who controls the Internet?Illusions of a borderless world*, Oxford, 2006, cap.4.
[129] I.KATZ, *Web freedom faces greatest threat ever, warns Google's Sergey Brin*, in *Guardian*, 15 aprile 2012, https://www.theguardian.com/technology/2012/apr/15/web-freedom-threat-google-brin (consultato il 25 febbraio 2019).

distinti profili; quello geografico, poiché nelle zone rurali o a basso sviluppo economico non sono presenti le adeguate infrastrutture per permettere alla popolazione di connettersi a Internet, e quello sociale, per incentivare una "cultura digitale" in maniera tale che ogni cittadino sia in grado di avere gli strumenti conoscitivi per navigare nel ciberspazio con cognizione di causa[130].

La possibilità di navigare nello spazio cibernetico è ormai un requisito basilare per l'inclusione sociale e per la partecipazione alla vita economica della propria comunità[131]: coloro che sono esclusi dal *cyberspace* non hanno modo di far sentire la propria voce, rischiando di scivolare in una sorta di oblio poiché non hanno la possibilità di comunicare e di ricevere informazioni[132]. Un simile "silenzio digitale" potrebbe comportare una violazione dei diritti umani di un individuo, rendendo perciò necessario che la disponibilità di una connessione Internet sia garantita dalla normativa vigente.

1.2.Ragioni contrarie al riconoscimento del diritto all'accesso a Internet come nuovo diritto fondamentale

Le reti digitali, secondo coloro che non riconoscono alcun carattere fondamentale al diritto all'accesso a Internet, sono da considerarsi meri strumenti tecnologici utilizzati per la realizzazione di ulteriori principi. Questa è l'opinione di Vint Cerf, co-inventore insieme a Bob Kahn del protocollo IP/TCP, indispensabile tutt'oggi per la navigazione sul *web*[133]. L'ideale di diritto umano/fondamentale che si è formato nella cultura occidentale fa sì che ogni persona può legittimamente reclamare l'adempimento di tali principi essenziali per la vita umana[134]. I suddetti principi, secondo la prospettiva giuridica classica, sono delle garanzie che vengono assicurate a qualsiasi essere umano,

---

[130] A.SEGURA SERRANO, *Internet regulation and the role of international law*, in *Max Planck Yearbook of United Nations Law*, vol.10, 2006, pp.264-270.
[131] A.POWELL, A.BRYNE, D.DAILEY, *The essential Internet: digital exclusion in low-income American communities*, in *Policy and Internet*, 2(2), 2010, pp.161-163.
[132] D.STEVENS, K.O'HARA , *Inequality.com: politics, power and digital divide*, Oxford, 2006, pp.86-87.
[133] V.CERF, *Internet access is not a human right*, in *New York Times*, 4 gennaio 2012, https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html (consultato il 20 febbraio 2019).
[134] S.GREER, *The European Convention on Human Rights. Achievements, problems and prospects*, Cambridge, 2006, p.2.

indipendentemente dalla sua provenienza geografica, culturale o dal suo status economico[135]. I diritti fondamentali sono perciò i valori che permettono all'essere umano di condurre una vita sana e piena di significato: che una connessione a internet sia indispensabile per raggiungere un simile traguardo può essere quantomeno contestabile.

Cerf sostiene che la tecnologia deve essere considerata come strumento per il raggiungimento, l'affermazione e la tutela di determinati diritti e non come diritto essa stessa. Prosegue segnalando una distinzione che merita di essere menzionata, ossia quella tra diritti fondamentali, intrinsecamente legati all'essere umano, e diritti civili, conferiti e riconosciuti attraverso la legge. L'accesso a Internet potrebbe rientrare in quest'ultima categoria secondo la visione di Cerf, poiché il voler garantire la connessione al *web* ai propri cittadini potrebbe far parte delle politiche intraprese da uno Stato. Un altro punto sollevato dall'inventore del protocollo IP/TCP per dimostrare la propria tesi è che Internet non è altro che un'invenzione tecnologica e che quindi verrà resa obsoleta dal progresso scientifico: un diritto fondamentale non dovrebbe cadere preda di un simile destino. Una possibile obiezione a quest'ultimo pensiero è data dal fatto che il termine "Internet" viene comunemente usato per indicare il mondo informatico in generale — comprensivo di siti *web*, mail, etc — e non la specifica tecnologia utilizzata per permettere la navigazione nello spazio cibernetico[136].

Spostando la riflessione su un piano più prettamente giuridico, è stato fatto notare[137] che, per qualificare un determinato principio come diritto fondamentale, occorre che questo sia riconosciuto da un Trattato internazionale che ne prescriva anche degli strumenti di tutela e giustiziabilità. Allo stato attuale, il diritto all'accesso a Internet è carente di tale requisito.

Non deve essere inoltre sottovalutato il rischio di "inflazionare" la categoria dei diritti fondamentali: acconsentire a ogni richiesta di riconoscimento per un nuovo diritto umano potrebbe infatti portare alla frammentazione della suddetta categoria[138] e a far

---

[135] J.NICKEL , *Making sense of Human Rights: Philosophical reflections on the Universal Declaration of Human Rights*, Los Angeles, 1987, p.22.

[136] T.BERNERS LEE, H.ALPIN, *Internet access is a human right*, https://www.ibiblio.org/hhalpin/homepage/publications/def-timbl-halpin.pdf (consultato il 20 febbraio 2019).

[137] O.POLLICINO, *Audizione del 24 febbraio 2015 presso la 1° Commissione Permanente (Affari Costituzionali) del Senato della Repubblica*, https://www.senato.it/application/xmanager/projects/leg17/attachments/documento_evento_procedura_commissione/files/000/002/446/prof._POLLICINO.pdf (consultato il 2 maggio 2019).

[138] F.H.EASTERBROOK, *Cyberspace and the law of the horse*, in *University of Chicago Legal Forum*, vol. 207, 1996, pp.3 ss.; L.LESSIG, *The law of the horse:what cyberlaw might teach*, in *Harvard Law Review*, vol.113 (2), 1999, pp.10 ss.

perdere di valore i diritti già esistenti. Si rischierebbe inoltre di vanificare le garanzie e le salvaguardie per i valori meritevoli di una maggiore protezione[139].L'inclusione di un nuovo principio nel novero dei diritti fondamentali è necessaria solo se comporta una maggiore protezione per l'essere umano rispetto a quella già in vigore e solo dove c'è un consenso unanime sulla necessità di una salvaguardia aggiuntiva.

Aggiungere un nuovo diritto all'elenco dei diritti fondamentali richiede inoltre un apposito intervento normativo che può però incontrare diversi problemi; occorre riflettere su quale strumento legislativo è necessario adottare e a quale livello delle fonti di produzione del diritto intervenire. Un ulteriore rischio da non trascurare è che tale intervento potrebbe diventare obsoleto[140].

1.3. Il diritto all'accesso a Internet può essere considerata una nuova norma consuetudinaria?

La rapida diffusione delle nuove tecnologie ha comportato conseguenze giuridiche da non trascurare, andando a influenzare gli ordinamenti di diversi Stati nazionali. Al fine di valutare se il diritto all'accesso a Internet può essere considerato come una nascente norma di diritto consuetudinario occorre perciò valutare l'effettiva importanza di tali conseguenze.

La realtà normativa internazionale attuale in materia di tutela della connessione al *cyberspace* è scarna e disomogenea; ben pochi Paesi, segnatamente la Spagna, il Costa Rica, la Francia, la Finlandia, l'Estonia e la Grecia hanno introdotto il diritto all'accesso a Internet all'interno del proprio ordinamento e attraverso diversi mezzi. La Corte Costituzionale francese ha posto il diritto a una connessione Internet sotto la protezione della Dichiarazione dei Diritti dell'Uomo e del Cittadino come parte della libertà di espressione[141]. La Costituzione greca è stata emendata per includere l'art.5A[142] che assicura a ogni cittadino del Paese il diritto a partecipare alla società dell'informazione, impegnando le autorità nazionali greche a garantire i mezzi necessari per raggiungere tale

[139] B.SKEPYS, *Is there a human right to Internet?*, in *Journal of Politics and Law*, vol.5, n.4, 2012, http://ccsenet.org/journal/index.php/jpl/article/view/22541 (consultato il 2 maggio 2019).
[140] C.KUNER, *An international legal framework for data protection: issues and prospects,* in *Computer law and Security Review*, vol.25(4), 2009, pp.307-317.
[141] Act furthering the diffusion and protection of creation on the Internet, Decisione n.2009-580 del 10 giugno 2009, Consiglio Costituzionale francese, https://www.conseil-constitutionnel.fr/sites/default/files/2018-10/2009_580dc.pdf (consultato il 17 aprile 2009).
[142] La Costituzione della Grecia, così come emendata dalla risoluzione parlamentare del 6 aprile 2001, https://www.wipo.int/edocs/lexdocs/laws/en/gr/gr220en.pdf (consultato il 17 aprile 2019).

scopo. La Finlandia si è spinta addirittura oltre, arrivando ad affermare che il diritto ad accesso a Internet deve essere considerato come fondamentale[143].

Nonostante le rare e difformi prese di posizione da parte dei diversi Stati, l'opinione comune, come testimoniato dal sondaggio commissionato dalla BBC a cui si accennava precedentemente, sembra ritenere che una connessione allo spazio cibernetico rientri nei diritti inalienabili dell'essere umano. Il parere del popolo non è certamente bastevole per far sì che una qualche tutela normativa venga garantita all'accesso a Internet, anche perché bisogna tenere in considerazioni due diversi elementi. *In primis*, la risposta al predetto sondaggio è stata data da coloro che già sono in possesso di una connessione al *web* e inoltre, come si è visto, la risposta degli Stati non può certo essere considerata come pratica comunemente accettata, secondo quanto previsto dall'art.38 dello Statuto della Corte di giustizia internazionale. Considerato ciò, è quantomeno prematuro affermare che il diritto all'accesso a Internet è una norma di diritto consuetudinario, non escludendo però che possa raggiungere tale *status* in futuro.

1.4. Riflessioni sulle possibili conseguenze dell'affermazione del diritto a Internet come fondamentale

Affermare il carattere fondamentale del diritto all'accesso a Internet è una presa di posizione non priva di conseguenze, sia giuridiche che socio-economiche. Le caratteristiche del mondo digitale[144], come la sua architettura diffusa senza alcun controllo centrale gerarchico, potrebbero favorire la libera connessione e l'inclusione del *cyberspace* nella categoria dei *global commons.* La mancanza di una qualsiasi sovrastruttura dovrebbe garantire la piena libertà degli utenti che sono in grado di diventare loro stessi produttori di contenuti non limitandosi al ruolo di meri fruitori come accade con i *media* tradizionali.

Con il termine *commons* si vuole solitamente indicare un insieme di comportamenti e di atteggiamenti considerati nel loro insieme, che rispettano 5 specifiche caratteristiche[145]: a) i partecipanti devono volontariamente aderire ai *commons*, senza

[143] Finland makes broadband a legal right, BBC news, 1 luglio 2010, https://www.bbc.com/news/10461048 (consultato il 17 aprile 2019).
[144] J.HOLMAN, M.MCGREGOR, *The Internet as commons: the issue of access,* in *Communication Law and Policy*, vol.10, n.3, 2005, pp.267-289.
[145] R.OAKERSON, *Analyzing the commons: a framework*, in (a cura di) D.W.BROMLEY, *Making the commons work: theory, practice and policy,* New York, 1992, pp.42 ss.

coercizione alcuna; b) gli utenti devono avere uno scopo comune prefissato; c) devono condividere le risorse messe a disposizione e le proprie azioni; d) la partecipazione deve essere caratterizzata da un atteggiamento di collaborazione; e) i rapporti sociali sono connotati dal rispetto reciproco.

L'afflato democratico[146] delle reti digitali si scontra però con la progressiva concentrazione delle fonti di produzione delle informazioni e di contenuti nelle disponibilità di poche grandi società di telecomunicazioni e dello spettacolo. In un mercato di stampo capitalistico, le suddette *corporation* hanno il potere di decidere di quali contenuti il singolo utente può effettivamente usufruire durante la sua navigazione nello spazio cibernetico, limitando quindi la sua libertà di informazione e allontanando il concetto di Internet come ambiente libero e senza ostacoli. Il diritto all'accesso viene subordinato al requisito del consenso[147]: il proprietario del materiale richiesto deve acconsentire al suo utilizzo da parte dell'internauta.

Internet, funzionando come una rete di *network*, espande le sue funzionalità con la connessione di nuovi utenti. La presenza di nuovi soggetti nell'ambiente cibernetico non porta al consumo delle risorse presenti, ma al loro incremento. Nuovi internauti possono infatti condividere nuove informazioni e contenuti nel *web.*

Considerare l'accesso a Internet come diritto fondamentale comporterebbe una regolamentazione dell'ambiente cibernetico nell'ottica dei *global commons*, favorendo la connessione universale in controtendenza rispetto alla situazione attuale che vede l'affermarsi di pochi grandi *player* nel mercato digitale.

Cambierebbe quindi il ruolo degli *Internet Service Provider* (ISP), ossia coloro che forniscono agli utenti servizi informatici come la connessione al *web*. Attualmente essi prendono decisioni unilaterali riguardo all'effettiva esperienza che gli internauti hanno navigando in rete, ma una simile circostanza non potrebbe verificarsi nel caso di una connessione universale senza limitazioni.

Un libero accesso a Internet non può però condurre alla condivisione di materiale illegale o offensivo sotto la giustificazione della libertà di espressione; i diritti fondamentali possono infatti subire delle restrizioni in caso di necessità, come si vedrà nel proseguio della trattazione.

---

[146] J.BERMAN, D.J.WITZNER, *Technology and democracy*, in *Social Research*, n.64, 1997, pp.1313-1315.
[147] O.S.KERR , *Cybercrime's scope: interpreting access and consent in computer misuse statutes',* in *New York University Law Review*, n.78, 2003, pp.1596.

2. La connessione a Internet come strumento per la realizzazione del diritto alla libera espressione nell'epoca digitale

Una delle funzioni principali di Internet è quella comunicativa; la rete informatica è nata per mettere in collegamento i diversi utenti connessi permettendo loro così di comunicare in tempo reale. L'avvento dei *network* digitali ha rovesciato il tradizionale meccanismo di circolazione delle informazioni[148], permettendo agli utenti di non ricoprire esclusivamente il ruolo di "destinatari finali" delle notizie che venivano indirizzate loro attraverso la mediazione degli operatori del settore come i giornalisti. Ora è possibile per ciascun individuo connesso allo spazio cibernetico far sentire la propria voce: pubblicando un *post* su un *social media*, scrivendo un *blog* o registrando e condividendo in rete un video.

La nuova epoca dell'informazione si caratterizza perciò per la sua struttura a rete[149], dove ogni utente è un potenziale produttore di notizie, anche grazie al prezzo relativamente basso di un *device* elettronico dotato di connessione a Internet. Un simile mutamento comporta anche delle implicazioni rilevanti di ordine giuridico che portano a riflettere sul concetto di diritto alla libera espressione nell'epoca digitale[150].

Il collegamento tra tale diritto e il libero accesso al *cyberspace* è stato più volte evidenziato anche da strumenti di *soft law* internazionale[151].

La scelta di ricorrere ad atti non vincolanti non è casuale; il carattere sovranazionale dello spazio cibernetico comporta infatti il coinvolgimento dell'intera comunità internazionale nella sua regolamentazione. Raggiungere l'unanimità in un consesso così ampio può essere assai complesso, considerati i diversi interessi in gioco. Risulta quindi preferibile, almeno per il momento, limitarsi a dichiarazioni di intenti e prese di posizione che non causino alcun obbligo giuridico. Gli unici documenti internazionali vincolanti[152] in tema di *cyberspace* sono la Convenzione delle Nazioni

---

[148] T.E.FROSINI, *op.cit.*

[149] Y.BENKLER, *The wealth of networks. How social production transforms markets and freedom*, Yale, 2006, p.10 ss.

[150] V.ZENO-ZENCOVICH, *Perché occorre rifondare il significato della libera manifestazione del pensiero*, in *Percorsi Costituzionali*, n.1, 2010, pp.69 ss.

[151] F.MARCELLI, *L'accesso a Internet come diritto fondamentale? Tendenze del diritto internazionale e realtà dei fatti*, in (a cura di) M.PIETRANGELO, *Il diritto di accesso a Internet*, 2010, Napoli, pp.99-108.

[152] M.R.ALLEGRI, *Riflessioni e ipotesi sulla costituzionalizzazione del diritto di accesso a Internet (o al ciberspazio?)*, in *Rivista dell'Associazione Italiana dei Costituzionalisti*, n.1/2016, 29 febbraio 2016, pp.1-31.

Unite sui diritti delle persone con disabilità[153], al cui art.9 viene sancito il diritto per i disabili di accedere alle nuove tecnologie e ai sistemi di informazione, e la Convenzione sul *Cybercrime*[154] stipulata in seno al Consiglio di Europa.

Il rapporto di La Rue a cui prima si accennava, dove Internet viene definito come il mezzo ideale per far sentire la propria voce nel pieno rispetto del diritto alla libertà di pensiero, è un chiaro esempio di questa tendenza ad utilizzare strumenti non giuridicamente vincolanti nella regolamentazione del diritto di opinione nel contesto cibernetico.

Non comporta obblighi giuridici nemmeno la Dichiarazione Universale dei Diritti Umani[155], stipulata in seno alle Nazioni Unite: l'art.19, ripreso quasi letteralmente dall'art.19 del Patto Internazionale sui Diritti Civili e Politici (ICCPR)[156], proclama il diritto alla libera espressione per qualsiasi individuo. Viene tutelato il lato sostanziale di tale principio, poiché si specifica che una persona ha la libertà di avere una propria opinione e di ricercare e diffondere informazioni e idee. La formulazione dell'art.19 sembra ritrarre anche la moderna realtà cibernetica, dove gli utenti collegati si scambiano in tempo reale contenuti di vario genere. Riceve parimenti tutela il mezzo di comunicazione; il medesimo articolo specifica infatti che la protezione è assicurata per qualunque strumento attraverso il quale l'espressione viene trasmessa e diffusa, sia essa in forma scritta, orale stampata o con qualsiasi altro metodo scelto dall'utente.

"*I membri della Commissione devono tenere in considerazione che il loro lavoro è rivolto verso il futuro e non verso il passato. Nessuno può prevedere come si evolveranno i mezzi di comunicazione nei secoli a venire."*[157] Il delegato francese si espresse così durante i lavori preparatori alla stesura del Patto Internazionale, discutendo l'utilizzo della parola *media* nella stesura dell'art.19; era già presente il pensiero di come

[153] Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, A/RES/61/106, 24 gennaio 2007, https://www.unicef.it/Allegati/Convenzione_diritti_persone_disabili.pdf (consultato il 16 aprile 2019)

[154] Trattato n.185, Convenzione sul *Cybercrime*, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (consultato il 16 aprile 2019).

[155] Il 10 dicembre 1948, l'Assemblea Generale delle Nazioni Unite approvò la Risoluzione 217 A (III) e proclamò la Dichiarazione Universale dei Diritti Umani, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/itn.pdf.

[156]Patto Internazionale sui Diritti Civili e Politici, Risoluzione 2200A (XXI) dell'Assemblea Generale delle Nazioni Unite, 16 dicembre 1966 https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (consultato il 16 aprile 2019).

[157]Consiglio per i Diritti Umani delle Nazioni Unite, sesta sessione, 165esimo meeting, 2 maggio 1950, http://hr-travaux.law.virginia.edu/document/iccpr/ecn4sr165/nid-1732 (consultato il 1 marzo 2019).

l'evoluzione dei mezzi di comunicazione avrebbe influenzato l'applicazione del diritto alla libera espressione negli anni seguenti.

Per permettere che ogni individuo possa effettivamente far sentire la propria voce, occorre infatti tutelare la libertà e l'accessibilità dei mezzi di comunicazione: l'art.19 dell'ICCPR, così come il suo equivalente nella Dichiarazione Universale, esplicitano la possibilità per ogni persona di utilizzare qualsiasi strumento (*media* nella stesura originale in lingua inglese) per diffondere e condividere le proprie idee e opinioni. L'elenco proposto non è quindi tassativo, ma lascia spazio a future innovazioni nel campo delle tecnologie di comunicazione. La Rue riteneva infatti che simili disposizioni fossero pienamente applicabili anche a Internet e ai nuovi *media*. Il Commentario delle Nazioni Unite sull'art.19 del Patto Internazionale sui Diritti Civili e Politici[158] afferma che le autorità nazionali devono tenere nella dovuta considerazione le evoluzioni tecnologiche che hanno radicalmente cambiato il modo di comunicare dal tempo in cui l'ICCPR fu scritto e ratificato.

Lo stretto legame tra il diritto alla libera espressione e il diritto all'accesso a Internet viene confermato[159] dall'applicazione della tecnica di interpretazione evolutiva[160] dei Trattati, secondo la quale ci sono occasioni in cui le parti contraenti hanno voluto dotare le parole utilizzate nella stesura del documento di un significato non fisso e stabilito, ma capace di evolversi nel tempo. Il contenuto dei diritti e degli obblighi stabiliti da un Tratto può quindi mutare nella sua portata con il corso degli anni.

Seguendo questa metodologia interpretativa, si può affermare che il diritto a Internet sia un risultato dell'evoluzione del più generale diritto alla libera espressione. A causa della relativa novità dell'avvento e della diffusione delle nuove tecnologie, la formulazione originaria dell'art.19 non poteva logicamente prendere in considerazione tali sviluppi. Date le numerose implicazioni che le reti digitali hanno nei confronti della libera espressione, si potrebbe ritenere che l'accesso a Internet meriti parimenti di essere tutelato a livello internazionale.

---

[158] Commentario delle Nazioni Unite sull'art.19 del Patto Internazionale sui Diritti Civili e Politici https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (consultato il 16 aprile 2019).

[159] A.SERGEEV, *The right to internet access: assessing the impact and the merits of compliance through an example of modern China,* in *International Journal of Law and Information Technology,* n.25, 2017, pp.309-335.

[160] Il concetto di interpretazione evolutiva venne delineato per la prima volta dalla Corte Internazionale di Giustizia nella sentenza *Navigational and Related Rights* del 13 luglio 2009.

Il diritto in questione non può però essere considerato assoluto[161], ma ammette interferenze da parte dei governi nazionali in difesa di superiori interessi pubblici. Specialmente quest'ultimo criterio rischia di lasciare un ampio margine di discrezionalità all'azione delle autorità nazionali che cercano un punto di equilibrio tra le necessità dell'intera comunità dei cittadini e il diritto del singolo[162]. Tale margine sarà inevitabilmente più ampio se andrà a coinvolgere argomenti ritenuti sensibili per l'opinione comune (si pensi a questioni religiose o etiche), mentre sarà più ristretto nell'ambito di argomenti su cui vige una sorta di consenso[163].

Ragioni relative alla stabilità e alla sicurezza nazionale sono spesso state utilizzate per giustificare misure di censura e di limitazione all'utilizzo di Internet, pur dovendo tali interferenze rispettare gli standard internazionali[164] ed essere proporzionali allo scopo prefissato.

Il diritto alla libera espressione non ha un valore assoluto nemmeno nel quadro normativo europeo, dove è invece suscettibile delle medesime limitazioni[165]. La Rue, nel report a cui prima si accennava, ha cercato di individuare casi in cui simili restrizioni possono considerarsi legittime; secondo la sua opinione possono essere censurati contenuti informatici relativi ad abusi su minori, *hate speech*, diffamazione, discriminazione razziale o religiosa. Pur essendo un elenco di circostanze astrattamente e idealmente condivisibile, non viene meno il margine di discrezionalità. Quello che può costituire legittima espressione di idee politiche negli Stati Uniti, può essere considerato illegittimo in Germania[166].

L'art.10 della Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali[167], così come l'art.11 della Carta dei Diritti Fondamentali dell'Unione europea[168], proclamano il diritto alla libertà di espressione, ma non si pronunciano sulla tutela dei mezzi di comunicazione. Tuttavia, una qualsiasi limitazione

---

[161] S.SHEERAN, N.RODLEY, *Routdlege Handbook of International Human Rights Law,* Routledge, 2014, pp.381-382.
[162] J.CHRISTOFFERSEN, *Fair balance: a study of proportionality, subsidarity and primarity in the European Convention of Human Rights,* Londra, 2009, pp.198 e ss.
[163] Y.SHANY, *Toward a general margin of appreciation doctrine in International Law,* in *European Journal of International Law,* n.16, 2005, pp.927 ss.
[164] Z.F.K.ARAT, *Human rights worldwide: a reference handbook,* Amsterdam, 2006, pp.68-69.
[165] O. DE SCHUTTER, *International human rights law,* Cambridge, 2010, pp.257 ss.
[166] Si fa riferimento a contenuti di matrice nazifascista; cfr. L.LESSIG, P.RESNICK, *Zoning speech on the Internet: a legal and technical model,* in *Michigan Law Review,* n. 98 (2), 1999, pp.10 e ss.
[167] Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali, 4 novembre 1950, https://www.echr.coe.int/Documents/Convention_ITA.pdf (consultato il 17 aprile 2019).
[168] Carta dei Diritto Fondamentali dell'Unione europea, 2000/C 364/01, 18 dicembre 2000, https://www.europarl.europa.eu/charter/pdf/text_it.pdf (consultato il 17 aprile 2019).

all'utilizzo di tali strumenti andrebbe a incidere anche sull'effettiva libertà di informazione; un'ingerenza sull'uso di Internet e delle reti digitali non farebbe eccezione[169].

La giurisprudenza della Corte europea dei diritti dell'uomo conferma questa visione[170]: nel caso *Jersild v. Danimarca*[171]i giudici di Strasburgo hanno riconosciuto che quanto sancito dalla Convenzione, pur essendo stato pensato per la carta stampata, si applica anche ai mezzi audiovisivi specificando che tali strumenti riescono a dare un ulteriore significato alle informazioni che contribuiscono a far circolare e che quindi meritano adeguata protezione.

Nelle sentenze *Oberschlick v. Austria*[172] e *De Haes e Gijsels v. Belgio*[173] la Corte ha specificato che la Convenzione non si limita a proteggere il contenuto delle espressioni, ma anche la forma in cui queste vengono trasmesse.

Il diritto alla libera espressione ha prevalentemente un carattere negativo, ossia fornisce una protezione contro le interferenze illecite da parte dei poteri statali: nei due casi recenti *Scarlet v. Sabam*[174] e *Sabam v. Netlog*[175] la Corte di giustizia dell'Unione europea ha analizzato la legittimità di un sistema di filtraggio delle comunicazioni elettroniche, volto a prevenire l'eventuale violazione del *copyright*. Un simile sistema avrebbe costituito una misura preventiva, applicabile indistintamente a tutti gli utenti, filtrando tutte le comunicazioni trasmesse dai *device* connessi alla rete e sarebbe stato in funzione per un periodo di tempo indefinito. Una volta identificato un contenuto in violazione del diritto alla proprietà intellettuale, il *software* avrebbe poi provveduto a bloccarne la successiva diffusione. In entrambi i casi i giudici della Corte hanno affermato che il diritto alla proprietà privata deve essere bilanciato con altri diritti come quello della libera iniziativa economica, della tutela dei dati personali e per l'appunto alla libera espressione. Proprio in relazione a quest'ultimo principio, la Corte ha specificato che

---

169 P.VAN DJIK, *Theory and practice of the European Convention of Human Rights,* Amsterdam, 2006, pp.783 ss.
170 P.DE HERT, D.KLOZA, *op.cit.*
171 Corte europea dei diritti dell'uomo, sentenza del 23 settembre 1994, *Jersild v.Danimarca*, ricorso n.15890/89.
172 Corte europea dei diritti dell'uomo, sentenza del 23 maggio 1991, *Oberschlick v.Austria,* ricorso n. 11662/85.
173 Corte europea dei diritti dell'uomo, sentenza del 24 febbraio 1997, *De Haes e Gijsels v.Belgio,* ricorso n.19983/92.
174 Corte di giustizia dell'Unione europea, sentenza del 24 novembre 2011, *Scarlet v. Sabam,* causa C-70/10, ECLI:EU:C:2011:771.
175 Corte di giustizia dell'Unione europea, sentenza del 16 febbraio 2012, *Sabam v. Netlog,* causa C-360-10, ECLI:EU:C:2012:85.

l'applicazione di un sistema di filtraggio come quello appena spiegato avrebbe comportato un *vulnus* alla libertà informativa, poiché anche contenuti legittimi avrebbe corso il rischio di essere censurati.

2.1. Il rapporto tra l'accesso a Internet e altri diritti fondamentali

Il libero accesso a Internet può ragionevolmente ricevere tutela facendo riferimento anche ad altri diritti fondamentali al di là del diritto alla libera espressione; il diritto alla privacy (art.8 della Convenzione), il diritto alla libertà di pensiero, coscienza e religione (art.9) e il diritto alla libertà di associazione (art.11). Sono diritti a carattere essenzialmente negativo che tutelano anche il loro metodo di realizzazione[176]. I collegamenti con il principio della libera espressione non si fermano a tali somiglianze; analizzando brevemente il diritto alla riservatezza e all'autonomia informativa, si può pensare al caso dell'utilizzo di *e-mail* e *social network*. Nei due casi *Sabam* precedentemente citati, la Corte di giustizia dell'Unione europea ha giustamente osservato che un'indebita ingerenza negli *account* di posta elettronica o nei profili personali dei *social media* degli utenti informatici potrebbe causare non solo una violazione della loro sfera privata, ma anche un ostacolo della loro libertà di espressione. Risulta infatti evidente che qualsiasi soggetto, consapevole del rischio di poter essere spiato dai poteri pubblici, non può sentirsi libero di comunicare le proprie idee senza remore.

3. Il libero accesso a Internet come diritto sociale

Il diritto all'accesso a Internet non ha esclusivamente una dimensione negativa, rintracciabile nella libertà del cittadino di potersi connettere alla rete digitale senza timore di dover subire ingiustificate ingerenze da parte dello Stato e dei pubblici poteri, ma ha anche un'accezione positiva.

Il concetto di cittadinanza è legato sempre più a doppio filo con il mondo virtuale; la rete Internet è uno dei canali di comunicazione principali tra la Pubblica Amministrazione e il singolo individuo. La diffusione delle nuove tecnologie e la

[176] P.DE HERT, D.KLOZA, *op.cit.*

crescente necessità di maggiore trasparenza nell'azione amministrativa sono due fenomeni concomitanti e interconnessi[177].

Il diritto all'accesso a Internet, proprio per la sua valenza sociale, si configura perciò come una pretesa soggettiva del cittadino a prestazioni pubbliche, alla pari di altri settori come istruzione, previdenza sociale o sanità[178]. Una pretesa che si configura nella richiesta di rimozione degli ostacoli, che possono essere di natura tecnica, economica, culturale e/o sociale, alla navigazione in rete, così come nella predisposizione delle infrastrutture tecniche e tecnologiche adeguate a garantire una connessione efficiente.

La necessità di un intervento dei pubblici poteri per garantire la disponibilità di una connessione *web* si riscontra anche nel già citato documento LaRue: il punto 85 del report chiarisce che gli Stati devono adottare una politica tale da assicurare a ogni cittadino la possibilità di navigare in Internet a condizioni accessibili. Il punto 87 prosegue aggiungendo che, ove sono presenti le infrastrutture tecnologiche necessarie, i Paesi devono impegnarsi a supportare iniziative volte a permettere l'accesso alle informazioni disponibili in rete anche agli elementi più in difficoltà della popolazione, come gli individui con disabilità.

La qualificazione del diritto all'accesso a Internet come diritto sociale[179] rivela però un problema di fondo, dato dall'effettiva impossibilità di descrivere in una singola norma giuridica l'intervento statale che sarebbe astrattamente richiesto per la realizzazione della connessione informatica universale. La regola rischierebbe di diventare obsoleta al momento stesso della sua redazione, a causa del continuo progresso tecnologico che rischia di far diventare inadeguati i provvedimenti richiesti dal testo normativo.

Occorre poi chiarire cosa si intende con "diritto all'accesso a Internet"; disponibilità di un computer o di un qualsiasi altro *device* atto al collegamento con la rete? Possibilità di usufruire delle infrastrutture tecnologiche come cavi, *server* e ripetitori? Ricevere un'adeguata educazione digitale?

La mancata chiarezza sulla natura del diritto all'accesso a Internet rimanda la sua determinazione in ogni caratteristica alla esclusiva volontà del legislatore[180],

---

[177] A.LE PAGE, *Libertés et droits fondamentaux à l'épreuve de l'Internet,* Parigi, 2002, pp.61 ss.
[178] T.E.FROSINI, *op.cit.*
[179] P.MARSOCCI, *Lo spazio di Internet nel costituzionalismo*, in *Costituzionalismo.it*, n.2/2011, pp.1-16; P.TANZARELLA, *Accesso a Internet: verso un nuovo diritto sociale?*, 3 settembre 2012, https://www.gruppodipisa.it/images/rivista/pdf/Palmina_Tanzarella__Accesso_a_Internet_verso_un_nuovo_diritto_sociale.pdf (consultato il 19 aprile 2019).
[180] M.R.ALLEGRI, *op.cit.*

comportando uno "sforzo di immaginazione" da parte dei giudici in sede di tutela giurisdizionale in caso di eventuali omissioni legislative[181]. I tribunali sarebbero infatti chiamati a garantire l'effettiva applicazione del diritto in questione, anche per le parti non compiutamente espresse dalla norma giuridica[182].

Non bisogna inoltre trascurare l'aspetto economico, poiché assicurare la connessione per ogni utente comporterebbe un notevole dispendio di risorse per il Paese.

3.1.La responsabilità degli Stati nel raggiungimento dell'obbiettivo della connettività universale

Per assicurare il pieno utilizzo di ogni funzionalità di Internet, deve essere assicurata per ogni utente la possibilità di connettersi allo spazio cibernetico. La Rue, nel suo report a cui si è più volte accennato nel corso della trattazione, specificava che è compito di ogni Stato adottare le misure necessarie per garantire la piena attuazione del diritto alla libera espressione, permettendo a ogni persona di accedere ai mezzi necessari per esprimere le proprie idee, incluso Internet.

Occorre riflettere su quali obblighi siano effettivamente in capo ai vari governi nazionali per il raggiungimento dell'ambizioso progetto della connettività universale.

Relativamente ai possibili provvedimenti tecnici da intraprendere, i cittadini possono richiedere allo Stato di coprire in maniera diffusa e omogenea il territorio nazionale con la lunghezza di banda (velocità e stabilità di connessione) adeguata a far sì che ogni utente non riscontri ostacoli tecnici di alcun tipo durante la sua navigazione[183].

Il primo riferimento giuridico è alla cd.teoria degli obblighi positivi in materia di diritti fondamentali[184]. Mentre gli obblighi a carattere negativo impegnano gli Stati a non interferire con l'esercizio da parte degli individui delle proprie libertà, quelli positivi richiedono un intervento da parte dei pubblici poteri. Il testo della stessa Convenzione individua alcuni ambiti in cui un Paese deve attivarsi per tutelare efficacemente alcuni specifici valori dei propri cittadini: l'art.2 impegna infatti lo Stato a *proteggere* il diritto alla vita e parimenti l'art.8 lo obbliga a *rispettare* il diritto alla privacy. L'art.6 (3)

---

[181] P.COSTANZO, *Miti e realtà dell'accesso a Internet. Una prospettiva costituzionalistica,* in *Consulta OnLine,* 17 ottobre 2012, http://www.giurcost.org/studi/Costanzo15.pdf (consultato il 19 aprile 2019).

[182] G.DE MINICO, *Diritti, regole e Internet,* in *Costituzionalismo.it,* 8 novembre 2011, http://www.costituzionalismo.it/articoli/393/ (consultato il 19 aprile 2019).

[183] G.DE MINICO, *Internet regole e anarchia,* Roma, 2012, pp.127 ss.

[184] A.MOWBRAY, *The development of positive obligations under the European Convention on Human Rights by the European Court of Human Rights,* Londra, 2004, pp.16 ss.

sancisce il dovere dello Stato di garantire assistenza legale nell'ambito dei processi penali alle persone che non possono permettersela.

La Corte europea dei diritti dell'uomo ha sviluppato nel corso degli anni una giurisprudenza particolarmente attenta al concetto di obbligo positivo, basando la sua interpretazione della Convenzione sul principio di effettività, nella maniera ritenuta più adatta a tutelare gli interessi dei singoli individui. La prima definizione di tale concetto, e l'inizio di questa linea interpretativa, si può trovare nella sentenza *Belgian linguistic case* del 1968[185].

L'ambito in cui la Corte è legittimata a pronunciarsi è esclusivamente quello relativo ai diritti riconosciuti e sanciti dalla Convenzione stessa: deve quindi trovare un collegamento tra l'intervento attivo richiesto allo Stato e uno specifico diritto affermato dalla CEDU che può essere anche quello con l'obbligo di tutelare la dignità umana sancito dall'art.1[186]. La teoria degli obblighi positivi in materia di diritti umani è ormai considerata parte integrante dei doveri sanciti dalla Convenzione[187]. La Corte europea dei diritti dell'uomo ha infatti specificato che la libertà di espressione non dipende esclusivamente dal dovere di evitare qualsiasi ingerenza ingiustificata da parte dei pubblici poteri, ma può anche richiedere l'adozione da parte dello Stato di misure attive[188]. Tale impegno consiste nel prendere le adeguate e proporzionate misure per assicurare la tutela dei diritti degli individui[189]. I giudici di Strasburgo sembrano far riferimento al concetto di obblighi positivi per ovviare a eventuali lacune della normativa nazionale. Un simile atteggiamento potrebbe aprire il campo al dovere per gli Stati di adottare misure concrete per garantire la connessione a Internet in attuazione dell'art.10 della Convenzione che, come ricordato precedentemente, sancisce il diritto alla libera espressione[190].

---

[185] Corte europea dei diritti dell'uomo, sentenza del 23 luglio 1968, *Belgian linguistic case*, ricorsi n. 1474/62, 1677/62, 1691/62, 1769/63, 1994/63 e 2126/64.
[186] P.DE HERT, D.KLOZA, *op.cit.*
[187] J.F. AKANDJI - KOMBE, *Positive obligations under the European Convention on Human Rights. A guide to the implementation of the European Convention on Human Rights,* in *Human Rights Handbook,* n.7, 2007, pp.5 ss.
[188] Corte europea dei diritti dell'uomo, sentenza del 6 maggio 2003, *Appleby et al. v. the UK,* ricorso n.44306/98.
[189] Corte europea dei diritti dell'uomo, sentenza del 9 dicembre 1994, *Lòpez Ostra v. Spain,* ricorso n.16798/90.
[190] P.DE HERT, D.KLOZA, *op.cit.*

4. *Il diritto all'accesso a Internet nell'ordinamento Ue: diritto fondamentale o servizio universale?*

Il 97% dei cittadini dell'Unione europea può sfruttare una connessione Internet alla velocità di navigazione di 2 Mbps, mentre circa l'83% dei nuclei familiari ha a disposizione la tecnologia per accedere allo spazio cibernetico direttamente dalla propria abitazione[191]. Il territorio europeo è quindi caratterizzato da una forte e diffusa connessione informatica, che ha rivoluzionato la vita dei cittadini europei sotto diversi aspetti.

La crescente importanza delle nuove tecnologie non è passata inosservata alle istituzioni europee: il Libro Bianco *Delors*[192] della Commissione europea sottolinea come la diffusione delle reti digitali possa favorire una sorta di economia della conoscenza, stimolando la crescita delle imprese con conseguenti benefici occupazionali per tutta la popolazione. Viene auspicata la creazione di una società dell'informazione aperta a tutti gli individui, attraverso apposite politiche sociali ed economiche volte a favorire l'accesso alle nuove tecnologie per ogni persona.

Nell'epoca dell'economia della conoscenza, l'informazione diventa la nuova moneta di scambio[193] e Internet il principale strumento attraverso il quale è possibile guadagnarla; il *web* è la piattaforma attraverso la quale il cittadino riesce a far sentire la propria voce all'interno della comunità di appartenenza. Coloro che sono "esclusi" da tale spazio sociale non possono usufruire appieno degli stessi diritti vantati da coloro che invece hanno a disposizione le tecnologie necessarie alla navigazione informatica. Il *digital divide*[194], ossia il divario tra chi ha accesso alle informazioni e chi no, è forse l'elemento maggiormente discriminante dell'era attuale.

La creazione di un mercato unico, la libera circolazione delle persone delle persone e dei lavoratori sono obbiettivi che presuppongono un contesto socio-economico

---

[191] Commission Staff Working Document accompanying the communication "Connectivity for a competitive Digital Single Market: towards a European Gigabit Society" SWD(2016)300, Bruxelles 14 settembre 2016, https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52016SC0300 (consultato il 24 aprile 2019).

[192] Libro Bianco, *Crescita, competitività e occupazione. Le vie e le sfide da percorrere per entrare nel XXI secolo,* COM_1993_0700_FIN, 5 dicembre 1993, https://publications.europa.eu/en/publication-detail/-/publication/4e6ecfb6-471e-4108-9c7d-90cb1c3096af/language-en (consultato il 24 aprile 2019).

[193] A.ALU, *Il diritto di accesso ad Internet nell'ordinamento europeo*, in (a cura di) M.R.ALLEGRI, G.D'IPPOLITO , *Accesso a Internet e neutralità della rete fra principi costituzionali e regole europee*, Roma, 2017, pp.93-109.

[194] S.BENTIVEGNA, *Disuguaglianze digitali. Le nuove forme di esclusione nella società dell'informazione*, Roma, 2009, pp.10 e ss.

uniforme, che non presenta differenze di sorta tra i propri attori. L'azione normativa europea è stata certamente più incisiva[195] di quella adottata da piattaforme *multi-stakeholder* come l'ITU, data la sua forza vincolante per i diversi Stati membri.

La base giuridica di tale intervento è rintracciabile negli artt.170 e ss. del Trattato sul Funzionamento dell'Unione europea, sotto il Titolo XVI rubricato come *Reti Transeuropee*, che elencano e disciplinano le condizioni necessarie per incentivare la nascita e lo sviluppo della società dell'informazione. Gli articoli in questione sottolineano che l'Unione europea, per assicurare lo sviluppo di mercati concorrenziali, deve agire per garantire un'efficiente rete di telecomunicazioni a livello transeuropeo, favorendo l'accesso a tale rete per tutti gli utenti. L'art.171 chiarisce che, per raggiungere tale obbiettivo, è necessaria la collaborazione degli Stati membri sotto la spinta coordinatrice dell'Unione stessa.

Un ruolo centrale viene svolto dalla Commissione europea, incaricata di promuovere piani per favorire la diffusione delle reti digitali e il loro accesso agli utenti; una Comunicazione del 1999 formulata da tale istituzione proclama che, per diventare l'economia più competitiva a livello globale, l'Unione europea deve sfruttare le opportunità date da Internet.[196] Una successiva Raccomandazione si concentra invece sulle misure necessarie a ridurre il divario digitale, avvertendo la necessità di incentivare l'alfabetizzazione informatica per dare la possibilità a ogni persona di vivere efficacemente la propria dimensione sociale[197]. Il 29 maggio 2010 è la volta di *Digital Agenda for Europe*[198], un elenco stilato sempre dalla Commissione di 101 azioni volte a realizzare 13 distinti obbiettivi in sette aree prioritarie per promuovere un mercato digitale unico.

Pur avendo riconosciuto a livello istituzionale in numerose occasioni il ruolo importante del *web* nella società attuale, il diritto all'accesso a Internet non è incluso tra i diritti fondamentali dell'Unione europea; come visto precedentemente, non se ne fa

---

[195] L.JASMONTAITE, P.DE HERT, *Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment?*, in *Research Handbook on Human Rights and Digital Technology*, Bruxelles, 2017, pp.157-179.

[196] Comunicazione dell'8 dicembre 1999, relativa ad un'iniziativa della Commissione in occasione del Consiglio europeo straordinario di Lisbona del 23 e 24 marzo 2000: eEurope - Una società dell'informazione per tutti, COM (1999) 687, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM%3Al24221 (consultato il 24 aprile 2019).

[197] Raccomandazione della Commissione, del 20 agosto 2009, sull'alfabetizzazione mediatica nell'ambiente digitale per un'industria audiovisiva e dei contenuti più competitiva e per una società della conoscenza inclusiva, in GU L 227, 29 agosto 2009, pp.9-12

[198] Comunicazione della Commissione del 26 agosto 2010, Un'Agenda Digitale europea, COM(2010) 245/2 DEF.

menzione né nella Carta né nella Convenzione. La pratica normativa nazionale, scarna e difforme, impedisce anche di considerare tale diritto come facente parte della tradizione costituzionale degli Stati membri[199].

Nonostante questo mancato riconoscimento formale, il quadro normativo europeo volto a disciplinare il mondo cibernetico si presenta variegato e ricco, soprattutto a livello di diritto derivato; il "pacchetto" di direttive adottate dal Parlamento e dal Consiglio il 7 marzo 2002 aveva infatti lo scopo di armonizzare le diverse disposizioni legislative nazionali favorendo al contempo adeguate condizioni di accessibilità alle reti digitali[200].

Gli ultimi anni hanno mostrato un crescente interesse dell'Unione europea al mondo cibernetico e alle funzioni sempre più fondamentali svolte da Internet nella società attuale.

Il Regolamento (UE) 2015/2120[201] stabilisce misure riguardanti l'accesso al mondo cibernetico da parte degli internauti, stabilendo che gli utenti hanno il diritto di accedere alle informazioni e ai contenuti presenti nel *cyberspace* nonché di utilizzare terminali e applicazioni di loro scelta in maniera indipendente da variabili quali la posizione geografica, la condizione economica o l'operatore che presta il servizio informatico richiesto. Il Regolamento ha reso perciò l'accesso a Internet un principio immediatamente applicabile all'interno del territorio dell'Unione europea, senza bisogno di ulteriori misure normative di recepimento nazionali[202].

4.1. La connessione al world wide web e la sua possibile regolamentazione come "servizio universale" secondo quanto affermato dalla direttiva 2002/22/CE

Le istituzioni europee hanno più volte dimostrato consapevolezza dell'importanza che la rete Internet ha nella società attuale; non solo sotto l' economico, ma anche come

---

[199] C.MCRUDDEN, *The future of European Charter of Fundamental Rights, Jean Monnet Working Paper n.10/01,* 18 marzo 2002, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=299639 (consultato il 24 aprile 2019).

[200] Si fa qui riferimento alla Direttiva "*accesso"* n.2002/19/CE, alla Direttiva "*autorizzazioni*" n.2002/20/CE, alla Direttiva "*quadro"* n.2002/21/CE e alla Direttiva "*servizio universale"* n.2002/22/CE.

[201] Regolamento (UE) 2015/2120 del Parlamento europeo e del Consiglio del 25 novembre 2015 che stabilisce misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione, in GU L 310, 26 novembre 2015, pp.1-18.

[202] M.R.ALLEGRI, *Una premessa, qualche considerazione introduttiva e qualche riflessione sul ciberspazio come ambiente di rilevanza giuridica,* in (a cura di) M.R.ALLEGRI, G.D'IPPOLITO, *op.cit.*, pp.7-25.

strumento di cittadinanza digitale. L'attenzione torna a focalizzarsi sull'aspetto più prettamente sociale del *web*, non visto esclusivamente come mezzo di comunicazione.

La nozione di "servizio universale", introdotta con la direttiva 2002/22/CE[203] può forse tutelare tale aspetto, impegnando gli Stati ad agire per garantire l'obbiettivo della connettività informatica globale. Il testo normativo indica con tale terminologia un "*insieme minimo definito di servizi di determinata qualità disponibile a tutti gli utenti a prescindere dalla loro ubicazione geografica, e tenuto conto delle condizioni specifiche nazionali, a un prezzo accessibile*". La corretta applicazione di tali servizi è posta a carico dei singoli Paesi, che ne devono assicurare gli standard qualitativi nel rispetto dei principi di obbiettività, trasparenza, non discriminazione e proporzionalità. La direttiva prosegue stabilendo all'art.4 che "*la connessione consente agli utenti finali di effettuare e ricevere chiamate telefoniche locali, nazionali ed internazionali, facsimile e comunicazioni di dati, a velocità di trasmissione tale da consentire un accesso efficace a Internet, tenendo conto delle tecnologie prevalenti usate dalla maggioranza degli abbonati e della fattibilità tecnologica*".

Il progresso nel settore delle telecomunicazioni continua a velocità sostenuta, costringendo il legislatore ad adeguare la normativa ai nuovi avanzamenti dell'informatica: la riforma del 2009[204] ha ammodernato la disciplina vigente, sottolineando il valore del diritto all'accesso a Internet come passo imprescindibile per la realizzazione dello "*spazio unico europeo dell'informazione"*[205]. Il *world wide web* viene riconosciuto come strumento essenziale per la libertà di espressione e per l'istruzione[206]; le uniche limitazioni alla navigazione informatica da considerarsi legittime sono quelle

[203] Direttiva 2002/22/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, in GU L 108 del 24 aprile 2002, pp.51-77.
[204] Si intende il Regolamento (CE) 1211/2009, la Direttiva 2009/136/CE e la Direttiva 2009/140/CE
[205] Art.1 della Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, in GU L 337, 18 dicembre 2009, pp.11-36.
[206] A.ALU, *op.cit.*

conformi alla CEDU e alla Carta[207] poiché il diritto all'accesso al *cyberspace* deve essere garantito a tutti gli utilizzatori a condizioni favorevoli e prezzi contenuti[208].

Ai fini della presente ricerca, volta a riflettere sull'effettiva natura del diritto all'accesso a Internet, occorre menzionare che l'art.3 *bis* della Direttiva 2009/140/CE introduce un meccanismo di protezione rafforzata per tutelare l'accesso alle nuove tecnologie di comunicazione che è simile a quello previsto dall'art.10 della CEDU a garanzia della libertà di espressione[209]. In maniera similare a quanto previsto dalla Convenzione, le limitazioni alla fruizione di Internet devono essere stabilite da apposite norme e devono rispettare il criterio di proporzionalità rispetto al fine perseguito.

L'intervento di riforma legislativa appena menzionato non ha però modificato alcunché per quanto riguarda la definizione di "servizio universale", che si basa ancora oggi sul parametro della diffusione della domanda[210]. Gli Stati hanno quindi il dovere di garantire una determinata prestazione solo se questa ha raggiunto già un ampio grado di diffusione all'interno della popolazione, al fine di evitare che la minoranza che ancora non ne usufruisce subisca una sorta di esclusione sociale. Il vizio di autoreferenzialità che affligge l'applicazione di detto parametro appare evidente; la norma, così come è formulata, si limita a riconoscere lo *status quo*, andando poi a disciplinare l'attuale utilizzo degli strumenti tecnologici senza tener conto dell'evoluzione e dello sviluppo della ricerca informatica. Considerato ciò, è auspicabile adoperare un criterio finalistico/teleologico, volto a valorizzare la necessità che dovrebbe essere soddisfatta dalla prestazione catalogata come "servizio universale", al posto di quello attualmente utilizzato della diffusività[211].

Stanti le attuali disposizioni normative, la tecnologia della banda larga, che permetterebbe agli utenti di navigare nello spazio cibernetico a una velocità maggiore rispetto a quella di cui usufruiscono attualmente, non può essere considerata "servizio

---

[207] Considerando n.4 della Direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica, in GU L 337, 18 dicembre 2009, pp. 68-100.

[208] Considerando n.22 della Direttiva 2009/140/CE.

[209] O.POLLICINO, *cit.*

[210] L.NANNIPIERI, *Costituzione e nuove tecnologie*, https://www.gruppodipisa.it/images/seminariDottorandi/2013/LORENZO_NANNIPIERI_Costituzione_e_nuove_tecnologie.pdf (consultato il 30 aprile 2019).

[211] G.DE MINICO, *Regulation, banda larga e servizio universale. Immobilismo o innovazione?*, in *Politica del Diritto*, n.4/2009, dicembre 2009, pp.531-566.

universale" data la sua relativamente scarsa diffusione. La connessione veloce rimane perciò un'opportunità che gli Stati possono concedere ai propri cittadini, ma non un impegno vincolante[212], a differenza dell'accesso a Internet che invece rientra nell'ambito del "servizio universale".

5. *Il diritto all'accesso a Internet e le esperienze politiche nazionali, con una particolare attenzione al caso italiano*

L'esperienza italiana in merito al diritto all'accesso a Internet può infatti ritenersi paradigmatica e riassuntiva delle diverse posizioni che sono state brevemente analizzate durante il presente studio. Sono state avanzate opinioni a favore della determinazione dell'accesso al *web* come diritto fondamentale, così come pareri che si soffermavano maggiormente sul carattere pubblico e sociale della disponibilità di una connessione al *cyberspace*. Lo studio delle varie prese di posizione della dottrina e delle proposte legislative che ne sono derivate può quindi essere utile per dare un ulteriore spunto di riflessione in merito alla reale natura del diritto all'accesso a Internet e di come può essere effettivamente disciplinato a livello europeo e internazionale.

L'origine del dibattito italiano a tal proposito può essere fatta risalire alle affermazioni di Stefano Rodotà durante i lavori dell'*Internet Governance Forum* del 2010, secondo il quale occorre inserire in Costituzione un art.21-*bis* che statuisce che ogni cittadino ha il diritto di accedere a Internet con strumenti tecnologici adeguati e che rimuovano ostacoli di natura sociale e/o economica[213]. Le parole del giurista italiano hanno ispirato un disegno di legge costituzionale[214].

Rodotà, pur consapevole del fatto che una legislazione statale si sarebbe rivelata presto inefficace a causa del carattere sovra-nazionale della rete cibernetica, bisognosa invece di una disciplina uniforme a livello internazionale, avvertiva comunque la necessità di ovviare alla mancanza di regolamentazione in materia di Internet, al fine di garantire comunque un'efficace tutela alle attività umane nel contesto cibernetico[215]. Non

---

[212] A.VALASTRO, *La garanzia di effettività del diritti di accesso a Internet e la timidezza del legislatore italiano*, in (a cura di) M.PIETRANGELO, *op. cit.*, pp.51 ss.
[213] Stefano Rodotà: ecco l'art.21-*bis*, quello del diritto a Internet, https://tv.wired.it/news/stefano-rodota-ecco-l-articolo-21-bis-quello-del-diritto-ad-internet.html (consultato il 6 maggio 2019).
[214] Disegno di legge costituzionale n.2845, https://www.senato.it/service/PDF/PDFServer/DF/232181.pdf (consultato il 6 maggio 2019).
[215] M.R.ALLEGRI, *Riflessioni e ipotesi sulla costituzionalizzazione del diritto di accesso a Internet (o al ciberspazio?), op.cit.*

è certamente casuale la scelta di numerare tale articolo come 21-*bis*, ancorandolo in maniera stretta e indissolubile all'art.21 che tutela la libertà di pensiero e di manifestazione. Internet viene quindi visto essenzialmente come un nuovo mezzo di comunicazione attraverso il quale le persone possono esprimere la propria opinione e far sentire la propria voce nella società digitale attuale. Una tale presa di posizione si scontra però con la giurisprudenza della Corte costituzionale italiana, che ha più volte ribadito che ad un diritto alla libera manifestazione non corrisponde parimenti la libera utilizzazione dei mezzi di comunicazione[216].

Il valore strumentale delle nuove tecnologie per la realizzazione di ulteriori principi fondamentali è alla base di un ulteriore tentativo di revisione[217] che prevede l'inserimento di un nuovo comma all'art.21, seguendo quindi la stessa linea di pensiero del disegno di legge costituzionale a cui precedentemente si accennava. Anche in questo caso si proclama il diritto dei cittadini a navigare in rete e a poter accedere alle informazioni ivi presenti, impegnando inoltre lo Stato a far sì che rimuova tutti gli ostacoli che impediscono l'accesso al *cyberspace*. Ritorna perciò la dimensione sociale del diritto a Internet, che si concretizza nella pretesa di un intervento attivo da parte dello Stato.

Tale aspetto si ripresenta chiaramente anche nella Dichiarazione dei diritti in Internet[218], frutto del lavoro di una commissione di ricerca formata da accademici e professionisti istituita dalla Presidenza della Camera dei Deputati. Il testo, pur essendo privo di forza prescrittiva e ricadendo quindi nell'ambito degli strumenti di *soft law*[219], riconosce il diritto fondamentale della persona a essere compiutamente informata per poter esprimere la propria opinione con cognizione di causa, ma auspica anche l'impegno dei pubblici poteri a garantire le tecnologie adeguate e a rimuovere qualsiasi ostacolo alla libera navigazione in rete.

Internet non svolge più una funzione esclusivamente comunicativa, ma è ormai diventato uno strumento indispensabile per la realizzazione del "cittadino digitale"[220]; il diritto all'accesso al *web* diventa perciò condizione imprescindibile per la realizzazione

---

[216] Tale principio è stato espresso più volte dalla Corte costituzionale italiana, a partire dalla sentenza 59 del 1960, http://www.giurcost.org/decisioni/1960/0059s-60.html (consultato il 7 maggio 2019).

[217] Disegno di legge costituzionale n.1317, http://www.senato.it/japp/bgt/showdoc/17/DDLPRES/0/751375/index.html (consultato il 7 maggio 2019).

[218] Dichiarazione dei diritti in Internet, http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf (consultato il 7 maggio 2019).

[219] M.R.ALLEGRI, *Riflessioni e ipotesi sulla costituzionalizzazione del diritto di accesso a Internet (o al ciberspazio?),op.cit.*

[220] S.RODOTÀ ,*Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione* , Roma-Bari, 2004, pp.94 ss.

di ulteriori diritti costituzionalmente garantiti, i quali altrimenti si troverebbero svuotati di significato nella società attuale[221], sempre più connessa e informatizzata, trovando una sorta di fondamento in quanto previsto dagli artt.2 e 3 della Costituzione italiana[222].

Questa consapevolezza ha portato a un ulteriore disegno di legge costituzionale[223] che propone una nuova *sedes materiae* per il diritto di accesso a Internet, ossia l'inserimento di un apposito art.34-*bis.* Il nuovo articolo, negli auspici dei proponenti, dovrebbe recitare che *Tutti hanno eguale diritto di accedere alla rete internet, in modo neutrale, in condizione di parità e con modalità tecnologicamente adeguate. La Repubblica promuove le condizioni che rendono effettivo l'accesso alla rete internet come luogo ove si svolge la personalità umana, si esercitano i diritti e si adempiono i doveri di solidarietà politica, economica e sociale»*. Risultano evidenti i richiami all'art.2 della Costituzione, specialmente nei termini di *personalità* e *solidarietà*[224]. La proposta in questione mette in risalto gli aspetti sociali e pubblici del diritto all'accesso a Internet, che non viene più considerato esclusivamente come una "semplice" libertà negativa, ma richiede un intervento pubblico a tutela e mantenimento delle condizioni minime di accesso al *cyberspace*[225]. Risulta infatti necessario che lo Stato agisca su due livelli distinti; uno più propriamente tecnico, ossia assicurare le infrastrutture necessarie al collegamento informatico, e uno più civile/culturale, investendo in programmi di formazione digitale per incrementare l'alfabetizzazione informatica e ridurre di conseguenza il *digital divide*. Non bisogna trascurare l'elemento economico: l'inserimento dell'art.34-*bis* in Costituzione comporterebbe inevitabilmente un notevole esborso per le casse dello Stato.

Ad oggi, nessuno dei progetti di legge presi in esame è ancora entrato in vigore. Il diritto all'accesso a Internet ha attualmente un riconoscimento costituzionale solo in Grecia e in Ecuador. L'art.5A comma 2 della Costituzione ellenica, così come revisionata nel 2001, prevede infatti che ogni cittadino ha il diritto di partecipare alla Società dell'Informazione e che, di conseguenza, lo Stato ha l'obbligo di agevolare l'accesso alle informazioni che circolano in forma elettronica, nonché la produzione, lo scambio e la

---

[221] V.F.MODUGNO, *I "nuovi diritti" nella giurisprudenza costituzionale*, Torino, 1995, pp.2 ss.
[222] P.COSTANZO , *I nodi della regolamentazione*, in *Diritto dell'Informazione,* n.4, 1999, pp.150 ss.
[223] Disegno di legge costituzionale n.1561, http://leg17.senato.it/service/PDF/PDFServer/BGT/00797423.pdf (consultato il 7 maggio 2019).
[224] M.R.ALLEGRI, *Riflessioni e ipotesi sulla costituzionalizzazione del diritto di accesso a Internet (o al ciberspazio?), op.cit.*
[225] G.D'IPPOLITO , *La proposta di un art.34-bis in Costituzione*, in (a cura di) M.R.ALLEGRI, G.D'IPPOLITO, *op.cit.*, pp.65-93.

diffusione di questi dati. La Costituzione dell'Ecuador entra più nello specifico, specificando che ogni persona, in forma individuale o collettiva, ha il diritto di accedere a parità di condizioni alle tecnologie dell'informazione, come le frequenze radio per la gestione di stazioni radiofoniche o televisive o le reti informatiche (art.16). Aggiunge inoltre che è compito dello Stato rendere effettivo tale diritto attraverso l'assegnazione delle frequenze radio e la creazione di reti di comunicazione, con particolare attenzione alle aree del Paese che sono carenti sotto tale punto di vista (art.17). A livello legislativo, tra i Paesi europei solo l'Estonia (dal 2000) e la Finlandia (dal 2009) hanno riconosciuto l'accesso a Internet come diritto soggettivo. Il Brasile ha approvato nel 2014 il Marco Civil da Internet[226]: una Carta dei Diritti *on-line* per i cittadini del Paese sudamericano. Il testo si propone di salvaguardare la libertà di espressione in rete (art.2) attraverso la tutela di principi quali la neutralità della rete, la protezione dei dati personali e la natura partecipativa di Internet. Ai fini della presente trattazione, è utile porre l'attenzione a cosa prevede l'art.8 del Marco Civil. Si afferma infatti che la privacy e la libertà di espressione sono valori imprescindibili per un pieno esercizio del diritto all'accesso a Internet. Si sostiene perciò il medesimo punto di vista di questa tesi, ossia che l'esperienza di navigazione in Internet di qualsiasi utente deve essere considerata nella sua interezza e non giudicata, *rectius* salvaguardata, attraverso un approccio a compartimenti stagni. I diritti rilevanti, quali la privacy, la libertà di espressione e l'accesso a Internet devono quindi coesistere in un uniforme quadro normativo in cui devono muoversi coerenti misure politiche e legislative.

6. Un diritto all'accesso ad una rete Internet neutrale. Il diritto all'uguaglianza cibernetica e la net neutrality

Il tema centrale della presente analisi è stato, fino a questo momento, il dibattito relativo all'effettiva natura del diritto alla connessione a Internet, ma occorre ora spostare l'attenzione su una domanda ineludibile per comprendere appieno la funzione di una connessione al *cyberspace* nell'epoca attuale: quali caratteristiche deve avere la rete su cui si vuole navigare? In altre parole: diritto all'accesso a quale tipo di Internet?

[226] Law 12.965, Marco Civil da Internet, https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180.

Il quesito non deve sembrare superfluo o prettamente tecnico-informatico, poiché il principio di uguaglianza insito nel diritto al *web* oggetto della presente trattazione non si esaurisce al momento dell'accensione del PC o di qualsiasi altro *device* atto a entrare nello spazio cibernetico, ma dovrebbe persistere per tutto il periodo dell'utilizzo da parte dell'utente. Il diritto all'accesso a Internet rischia di essere svuotato di ogni significato qualora l'individuo, pur potendo effettivamente connettersi al *web*, non possa effettivamente fruire liberamente di ogni contenuto e informazione ivi presente. L'analisi fino ad ora svolta si è concentrata sull'aspetto più propriamente tecnico dell'accesso a Internet, ossia la concreta ed effettiva disponibilità per ogni individuo delle infrastrutture necessarie per poter connettersi alla rete informatica. L'attenzione era perciò rivolta all'eventuale sussistenza in capo allo Stato di eventuali obblighi nei confronti della cittadinanza a tal proposito, senza indagare la realtà dei contenuti che effettivamente sono poi disponibili per la fruizione degli utenti nel contesto cibernetico. A tal proposito occorre perciò chiedersi se qualsiasi soggetto connesso al *cyberspace* ha le medesime opzioni di navigazione e di scelta tra le informazioni disponibili in rete o sussistono invece delle disparità date da ostacoli di carattere tecnico, normativo, sociale o economico. Risulterebbe infatti pressoché inutile garantire l'accesso a allo spazio cibernetico a qualsiasi cittadino, ma non la stessa esperienza di navigazione. Il diritto all'accesso a Internet risulterebbe infatti privato della propria essenza. Il *cyberspace* si sta affermando sempre più come una dimensione alternativa alla realtà concreta di ogni giorno, dove i nostri *alter ego* virtuali stringono rapporti e compiono azioni di ogni tipo. I dati personali e le informazioni che vengono condivise nell'ambiente virtuale sono elementi identificativi della persona a cui si riferiscono; considerato ciò, se non può essere tollerata la discriminazione di un individuo, perché sarebbe da ritenersi lecito discriminare i suoi dati[227]? Non vi è ragione per ritenere che l'applicazione del principio di uguaglianza non trovi spazio anche nel mondo *on-line*, limitandosi invece alla realtà strettamente fisica. Il dato è diventato un elemento fondante della personalità che merita adeguata tutela: il diritto all'*habeas corpus* si è evoluto nell'*habeas data*[228].

L'economia e la società attuale hanno sempre più legami con il contesto digitale e, di conseguenza, aumenta a ritmo incessante la richiesta di servizi informatici sempre

[227] G.D'IPPOLITO, *Neutralità della rete e uguaglianza: dallo stato di natura al diritto*, in (a cura di) P.PASSAGLIA, D.POLETTI , *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa, 2016, pp.325-337.
[228] S.RUSSO, A.SCIUTO, *Habeas data e informatica*, Milano, 2011;T.E.FROSINI, *Libertè, egalitè, Internet*, Napoli, 2015, pp.20 e ss.; G.D'IPPOLITO , *ibidem*.

più performanti: le reti di nuova generazione, che permettono una connessione a Internet più veloce e stabile, sono indispensabili per fruire di contenuti come i videogiochi *on-line*, per poter guardare film e video in *streaming*, per poter utilizzare applicazioni di *file-sharing* e per poter gestire in maniera efficace il traffico informatico. La particolare struttura della rete Internet permette l'esistenza separata di due tipi di operatori[229], ossia le grandi compagnie di telecomunicazione, che si occupano di predisporre e offrire le infrastrutture necessarie alla connessione *web*, e i cosiddetti operatori *over the top*, come Google, Facebook, Microsoft, Apple etc., che offrono servizi e contenuti attraverso dette infrastrutture senza però esserne effettivamente proprietari. Agiscono quindi "sopra la rete", traducibile per l'appunto in lingua inglese con la terminologia *over the top*.

Le compagnie di telecomunicazioni, al fine di garantire l'efficienza del proprio operato e far sì che non si creino "ingorghi" nel traffico informatico, si trovano spesso a dover applicare pratiche di *traffic management*. Tali azioni possono consistere ad esempio nel *traffic policing* (interruzione della connessione alla rete dopo che si è oltrepassata una determinata quantità di dati scaricati) o nel *traffic shaping* (redistribuzione del traffico nei lassi di tempo in cui vi sono meno richieste di connessione) e possono portare a trattamenti discriminatori nei confronti delle varie categorie di utenti.

L'uguaglianza cibernetica è ciò che è alla base del concetto di *net neutrality*, o neutralità della rete. Tale terminologia vuole indicare *"la parità di trattamento dei dati veicolati in rete e la facoltà degli utenti di accedere liberamente ai contenuti, servizi e applicazioni di propria scelta"*[230]. Nel corso degli anni si sono succedute numerose definizioni di tale concetto; una delle più famose, formulata da Tim Wu, afferma che con *net neutrality* si intende un principio di assoluta non discriminazione: il *network* di comunicazioni dovrebbe essere costruito in maniera tale da non privilegiare alcun contenuto trasmesso attraverso la propria rete a discapito di altri[231]. L'idea alla base di una rete neutrale è che ogni *bit*[232] è uguale all'altro e meritevole della stessa tutela; un

---

[229] A.ANANASSO, F.ANANASSO, *La neutralità della rete. Problematiche e aspetti regolamentari,* in (a cura di) M.R.D'ALLEGRI, G.D'IPPOLITO, *op.cit.*, pp.109-127.

[230] AGCOM, Delibera n.714/2011, *La neutralità della rete: pubblicazione delle risultanze della consultazione pubblica di cui alla delibera n.40/11/CONS,* https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=26154&content=La+neutralit%C3%A0+della+rete:+pubblicazione+delle+risultanze+della+consultazione+pubblica+di+cui+alla+delibera+n.+40/11/CONS&content_author= (consultato l'8 maggio 2019).

[231] T.WU, *Network neutrality broadband discrimination,* in *Journal on Telecommunications and High Technology Law*, vol.2, 2003, pp.141-176.

[232] Il termine *bit* indica la più piccola unità di dati nella memoria informatica. Risulta essere l'abbreviazione di *binary digit* e può avere esclusivamente valore di 0 o 1. Cfr. https://dictionary.cambridge.org/dictionary/english/bit (consultato l'8 maggio 2019.

simile pensiero è stato però fortemente criticato per diversi ordini di motivi. Secondo le voci contrarie alla *net neutrality*, non si può sostenere l'uguaglianza di ogni informazione: un *bit* trasmesso per visualizzare un video non può essere trattato allo stesso modo di uno trasmesso da un *peacemaker* impiantato nel cuore umano[233].

Un elemento di discriminazione può essere rinvenuto non solo a livello di rete, ma anche nei comportamenti tenuti dalle piattaforme *on-line*[234]: i *social media*, i motori di ricerca, i siti di *e-commerce* sono solo alcuni esempi di portali informatici che decidono in maniera autonoma quali contenuti mostrare all'utente, spesso ignaro dei complessi calcoli algoritmici che stabiliscono quali informazioni devono essere condivise con il potenziale consumatore. Tali piattaforme valutano il comportamento dell'individuo attraverso specifici fattori, come ad esempio quali prodotti acquista e a quali invece non è interessato, per poi classificarlo in uno specifico *ranking* ed offrirgli il bene/servizio che viene ritenuto più di suo gradimento. In tal modo, l'esperienza dell'utente A potrebbe essere completamente differente rispetto a quella della persona B, vanificando i principi di uguaglianza e neutralità della rete.

Il trattamento differenziato dagli utenti è però inevitabile, considerato il sistema di mercato attuale di stampo capitalistico; le grandi compagnie del settore delle telecomunicazioni hanno ogni interesse ad offrire servizi specifici a chi è disposto a pagare il prezzo richiesto. Tale atteggiamento può essere visto anche come uno strumento di "evoluzione economica"[235]: i consumatori con più alta disponibilità economica contribuiscono a finanziare anche la domanda di coloro che non possono permettersi il servizio più costoso.

Il ruolo del regolatore in tale ambito si rivela assai importante; lo scopo è trovare un punto di equilibrio tra due interessi apparentemente inconciliabili[236]; da una parte le dinamiche competitive di un mercato in cui sono presenti diversi operatori che offrono servizi e contenuti diversi a prezzi differenti e variegati, dall'altra la tutela da potenziali discriminazioni per i consumatori. L'obbiettivo di garantire la parità di trattamento all'utente finale può essere raggiunto solo se vengono tenute in debita considerazione le istanze di tre diversi gruppi di soggetti[237] a) gli utenti che devono essere in grado di

[233] N.NEGROPONTE, *Net neutrality doesn't make sense,* https://bigthink.com/videos/bits-bits-everywhere-with-mit-media-labs-nicholas-negroponte (consultato l'8 maggio 2019).
[234] A.ANANASSO, F.ANANASSO, *op.cit.*
[235] A.NICITA, *La neutralità della rete tra prospettive regolatorie e dilemmi irrisolti*, in (a cura di), M.R.D'ALLEGRI, G.D'IPPOLITO, *op.cit.*, pp.135-143.
[236] A.NICITA, *ibidem.*
[237] A.NICITA, *ibidem.*

usufruire dei servizi di connessione a Internet e di navigare nello spazio cibernetico senza essere sottoposti a ingiuste limitazioni; b) i fornitori di servizi e contenuti, anche detti operatori *over the top*, che, in un'ottica di mercato concorrenziale, devono avere la possibilità di offrire esperienze sempre più performanti e a buon prezzo; c) le TelCo, ossia le grandi compagnie di telecomunicazioni, che dispongono delle infrastrutture fisiche e tecnologiche necessarie.

6.1. Il diritto all'accesso a Internet e la net neutrality nel Regolamento (UE) 2015/212

La comparsa degli operatori *Over the Top*[238] e il loro progressivo dominio del mercato informatico ha portato l'Unione europea a dover ripensare la propria normativa in materia di telecomunicazioni informatiche, per adeguarla a un nuovo contesto economico. Il Regolamento (UE) 2015/2120 si prefigge l'ambizioso obbiettivo di garantire una rete informatica aperta all'insegna del principio della neutralità della rete agendo sotto due aspetti: da una parte sui rapporti tra ISP (*Internet Service Provider*) e gli altri operatori del settore informatico-digitale e dall'altra tutelando i cittadini e consumatori[239].

L'art.3 par.3 del Regolamento prevede che il traffico dati deve essere trattato in maniera equa, senza restrizioni, ingerenze o discriminazioni per quanto riguarda il contenuto o l'utente che lo ha condiviso. Sono però previste delle eccezioni e delle deroghe di cui deve essere fatta menzione. L'ISP può apportare delle procedure *ragionevoli* di gestione del traffico, nell'ottica di evitare congestioni e ingorghi che andrebbero a penalizzare i singoli consumatori nella fruizione del servizio offerto. Le misure devono essere trasparenti e proporzionate alla finalità espressa, senza influire sui contenuti trasmessi e rispettando quindi quanto previsto dalla Carta e dalla CEDU in materia di diritto alla libera espressione. La gestione *irragionevole* del traffico dati, ossia per finalità commerciali, è generalmente vietata e può essere applicata dall'ISP solo a specifiche e tassative condizioni. Ciò può accadere nella necessità di rispettare obblighi derivanti dal diritto dell'Unione europea, per preservare l'integrità della rete, dei terminali e delle infrastrutture o per prevenire una congestione della rete.

[238] Con tale terminologia si intende l'offerta di servizi multimediali direttamente all'utente finale attraverso Internet, senza l'utilizzo di intermediari di sorta.
[239] M.OROFINO, *La declinazione della net neutrality nel Regolamento europeo 2015/2120. Un primo passo per garantire un'Internet aperta?*, in *Federalismi.it*, n.2/2016, pp.2-25.

La normativa sembra lasciare un ampio spazio di interpretazione; cosa debba intendersi con i termini *ragionevole* e *irragionevole* deve essere valutato caso per caso, anche a seconda delle evoluzioni tecnologiche e degli strumenti di intervento concretamente disponibili. Resta fermo il principio di uguaglianza e di trattamento paritario dell'utente finale; consumatori che richiedono il medesimo servizio devono essere trattati alla stessa maniera.

L'art.3.5 del Regolamento prevede che gli ISP hanno la possibilità di offrire servizi *ottimizzati* di connessione per quei contenuti che richiedono una maggiore banda e una navigazione più stabile e duratura. Per far ciò, gli ISP devono però garantire una rete che sia in grado di supportare tali prodotti aggiuntivi che non devono in alcun modo essere sostitutivi di quelli basilari ed essenziali. In altre parole, l'offerta dei servizi ottimizzati non deve andare a discapito del comune accesso a Internet per gli utenti finali[240]. La disposizione normativa vuole evitare che gli operatori del settore, per fornire tali servizi a un guadagno presumibilmente maggiore, non trovino più profittevole continuare a garantire il semplice accesso a Internet alla platea degli utenti.

Proprio a questi ultimi intende rivolgersi il Regolamento, garantendo loro specifici diritti. *In primis* quello di accedere e diffondere informazioni attraverso Internet e le nuove tecnologie. Tali mezzi possono essere utilizzati anche per fornire contenuti, servizi e applicazioni: si vuole perciò tutelare anche la libera iniziativa economica del singolo soggetto. Sono inoltre vietate discriminazioni basate sul terminale e sulle apparecchiature utilizzate per accedere a Internet.

Il Regolamento investe di un ruolo di grande importanza le Autorità nazionali di garanzia in materia di telecomunicazioni; queste hanno infatti compiti di vigilanza, attuazione e di report nei confronti della Commissione europea.

6.2. La net neutrality nell'esperienza statunitense

L'approccio statunitense alla questione della *net neutrality* presenta sostanziali differenze rispetto a quello europeo che sono meritevoli di menzione. La prima normativa in tema di neutralità della rete è datata 1848 ed è stata emanata dallo Stato di New York[241]: prevedeva che gli operatori telegrafici non potessero privilegiare un determinato traffico

[240] M.OROFINO, *ibidem.*
[241] *An Act to provide for the incorporation and regulation of Telegraph Company*, 12 aprile 1848, *Laws of the State of New York*, chapter 340, pp.739 e ss.

dati rispetto a un altro sulla base del contenuto trasmesso. Questo primo atto ispirò la successiva legislazione statale e federale statunitense, che ancora oggi si basa sul principio del *first come, first served*, secondo il quale l'utente non deve essere in alcun modo discriminato in base all'origine della chiamata telefonica o dell'accesso a Internet e del contenuto della comunicazione[242].

6.2.1. La qualificazione degli Internet Service Provider come common carriers

Il legislatore americano, al fine di evitare qualsiasi discriminazione tra utenti intenzionati a navigare in Internet, si è trovato a dover riflettere sulla possibile qualificazione degli ISP come *common carriers*, intendendo con tale terminologia le compagnie impegnate a fornire alla comunità servizi pubblici di comunicazione. Solo gli operatori che rientrano in tale categoria sono infatti soggetti all'obbligo di non discriminare i consumatori in base alle variabili summenzionate. Il dibattito in merito a tale possibile catalogazione era reso ancora più complesso dall'aumento di attori *over the top*, impensabili all'epoca dell'emanazione del *Communications Act*[243] che nel 1934 disciplinò per la prima volta il settore delle comunicazioni a livello federale introducendo per l'appunto la nozione di *common carriers.* Il *Telecommunications Act* del 1996 introdusse la nozione di *Information Services* per distinguere coloro che si limitavano a fornire contenuti e informazioni dagli operatori che invece erano impegnati a predisporre le strutture di telecomunicazione.

Una lunga e travagliata vicenda giuridica e giudiziale ha portato a conclusioni significative[244]. La banda larga è stata classificata come *common carriage*, ossia servizio di pubblica utilità e la rete Internet è stata catalogata come appartenente al settore delle telecomunicazioni. Le norme statunitensi imponevano alle Telco di non operare alcuna degradazione del traffico informatico in merito ai contenuti trasmessi o alle applicazioni utilizzate (*no throttling)*, di non ricorrere ad alcun blocco delle informazioni lecite

[242] M.OROFINO, *ibidem.*
[243] *Communications Act of 1934*, https://transition.fcc.gov/Reports/1934new.pdf (consultato il 10 maggio 2019).
[244] Open Internet Order, https://www.fcc.gov/document/fcc-releases-open-internet-order (consultato il 10 maggio 2019).

condivise via *web* (*no blocking*) e di non garantire alcuna "corsia preferenziale" per i servizi e i contenuti a pagamento (*no priorization*).

La differenza principale tra la disciplina americana e quella Ue è data dalla diversa qualificazione che viene data alla connessione a Internet: la nozione di *common carriage* è diversa da quella di servizio universale utilizzata in territorio europeo. In quest'ultimo caso lo Stato nazionale non si limita infatti a disciplinare l'erogazione del servizio, ma può anche intervenire in prima persona per garantirne il funzionamento, in parziale deroga al divieto di aiuti di Stato[245].

Per concludere l'analisi dell'esperienza americana, occorre segnalare che l'amministrazione Trump ha cancellato la normativa *Open Internet Order,* riportando sostanzialmente in auge la disciplina previgente. L'opposizione democratica ha recentemente sostenuto e fatto approvare dalla Camera dei Rappresentanti un atto normativo che riporterebbe in vigore la regolamentazione prevista sotto la presidenza Obama. Attualmente tale atto è fermo in esame al Senato.

7. Riflessioni conclusive

Al termine di questa breve analisi, è opportuno proporre alcune osservazioni conclusive in merito al dibattuto tema della natura del diritto all'accesso a Internet.

Il ruolo del *world wide web* nell'epoca attuale non può essere più relegato semplicemente a mero mezzo di comunicazione; attraverso le nuove tecnologie di comunicazione una persona può compiere innumerevoli attività di carattere sociale, culturale ed economico. Il *cyberspace* è una dimensione dove i cittadini si incontrano, si informano, scambiano idee e opinioni e stringono rapporti di ogni tipo, sia con altri privati che con i pubblici poteri. La disponibilità di una connessione a Internet è un elemento importante per sfruttare efficacemente ogni opportunità di partecipare alla vita sociale e politica della propria comunità.

Considerato ciò, è corretto affermare che il diritto all'accesso a Internet è un nuovo diritto fondamentale? Trovare una risposta a questa domanda è stato l'obbiettivo principale del presente capitolo. Le posizioni in merito a tale dibattito sono ampie e articolate: voci autorevoli sostengono il carattere primario e assoluto di tale diritto dato che, come precedentemente accennato, le tecnologie informatiche sono adesso uno

[245] M.OROFINO, *op.cit.*

strumento indispensabile per la realizzazione della cittadinanza digitale, e opinioni altrettanto meritevoli di attenzione sostengono proprio che Internet non è altro che uno strumento per la realizzazione di ulteriori diritti autonomi e non un diritto a sé stante.

Una breve analisi della normativa internazionale ha rivelato che attualmente non esiste alcun Trattato vincolante che affermi o da cui possa desumersi la natura di diritto fondamentale dell'accesso a Internet, ma solo alcuni documenti di *soft law*. La prassi giuridica a livello nazionale si presenta inoltre assai difforme e variegata; alcuni Paesi hanno deciso di inserire all'interno del proprio ordinamento tale diritto, ma sono attualmente un'esigua minoranza. Non si può quindi riconoscere la formazione di una norma consuetudinaria a tal proposito, mancando per l'appunto sia il carattere della *diuturnitas* (Internet è ancora un fenomeno relativamente recente) che dell'*opinio juris ac necessitatis* (la maggioranza degli Stati non ha alcuna norma a tal proposito).

Per formulare una prima conclusione, il diritto all'accesso a Internet non può essere attualmente definito come diritto fondamentale, mancandone i presupposti giuridici. Non si rinviene infatti alcuna previsione esplicita a riguardo, né sono stabiliti mezzi di tutela giurisdizionale per tale supposto diritto. Non è certamente da escludere che la connessione al *web* raggiunga entro breve tempo tale *status*, specialmente considerando l'importanza di Internet nell'epoca moderna e l'avvertita esigenza di una sua salvaguardia come rete libera, indipendente e accessibile, ma non è ancora questo il momento.

Pertanto, le tecnologie informatiche possono essere considerate strumenti adeguati per l'esercizio di ulteriori diritti autonomi, come quello alla libera espressione.

La presente analisi ha seguito questa linea di indagine, soffermandosi su Trattati internazionali come la Dichiarazione Universale dei Diritti Umani e il Patto Internazionale sui Diritti Civili e Politici. L'art.19 di entrambi i documenti riconosce il diritto alla libera espressione attraverso ogni mezzo scelto dall'utente. La scelta intenzionale di non proporre un elenco tassativo degli strumenti utilizzabili per comunicare informazioni lascia intendere come tali disposizioni possano essere attuali anche nel contesto digitale.

Come osservato più volte, Internet non ha più una funzione esclusivamente comunicativa svolgendo anche un ruolo importante nella realizzazione del cittadino all'interno della propria comunità. A tal proposito, l'accesso al *web* non può essere considerato come una mera libertà negativa, concretizzabile ossia nella pretesa della

persona di non subire ingerenze e restrizioni da parte di terzi o dai pubblici poteri nell'esercizio di tale libertà, ma si afferma come diritto sociale.

Il cittadino vanta infatti una pretesa nei confronti dei pubblici poteri affinché questi si attivino su due distinti versanti: uno più prettamente tecnologico che consiste nel fornire gli strumenti e le infrastrutture necessarie alla connessione Internet, e uno sociale che si concretizza nel garantire alla popolazione l'adeguata alfabetizzazione e cultura digitale.

La qualificazione dell'accesso a Internet come diritto sociale rivela però delle problematiche di fondo. Una norma basata su tali presupposti rischierebbe di diventare obsoleta entro breve tempo: il costante progresso tecnologico potrebbe infatti rendere velocemente inadeguati gli interventi previsti a carico dei pubblici poteri. Non bisogna inoltre trascurare l'ampio potere di determinazione che avrebbe il legislatore in tale evenienza; sarebbe suo compito determinare l'*an* e il *quantum* di tale diritto. Si vuole intendere, ad esempio, quali investimenti fare, quali infrastrutture garantire per la connessione Internet. Paesi con diverse disponibilità economiche garantirebbero quindi possibilità diverse di accedere a Internet, a discapito di un approccio uniforme.

Il carattere sociale del diritto al *web* si ritrova anche nella normativa europea: la Direttiva 2002/22/CE ha infatti classificato la connessione al *cyberspace* come "servizio universale". Tale terminologia vuole indicare un insieme minimo di prestazioni che devono essere rese disponibili da parte dello Stato a tutti i cittadini ad almeno uno standard qualitativo minimo prefissato.

Il principio di uguaglianza alla base del diritto all'accesso a Internet rischia però di essere svuotato di significato se viene impedito al singolo utente di fruire di ogni contenuto presente nello spazio cibernetico. A tal proposito, entra in gioco il concetto di neutralità della rete: un *network* dove ogni informazione è trattata allo stesso modo di qualsiasi altra. Applicare tale valore al *web* attuale richiede però un'adeguata riflessione. Le grandi compagnie di telecomunicazione che si occupano di gestire le connessioni a Internet devono spesso ricorrere a pratiche di gestione del traffico informatico, al fine di evitare congestioni e collassi della rete. Non bisogna inoltre trascurare l'aspetto economico; gli ISP adottano discriminazioni tra i contenuti che offrono nell'ottica di ottenere un legittimo profitto.

L'approccio europeo alla questione della *net neutrality* è caratterizzato da una visione concreta e prettamente tecnica, priva di preconcetti ideologici. L'Unione europea ha infatti riconosciuto il valore di una rete Internet aperta e neutrale come presupposto

imprescindibile per un'efficace applicazione della libertà di espressione, ma non ha trascurato le esigenze degli operatori del settore tecnologico. Le grandi compagnie di telecomunicazioni possono infatti operare pratiche di gestione del traffico dati per prevenire "ingorghi" con conseguente detrimento per gli utenti e per privilegiare servizi specializzati ritenuti di particolare valore, a patto che questo non comporti discriminazioni ingiustificate per i consumatori.

Si ritiene, in conclusione, che l'accesso a Internet non può essere ancora considerato un diritto fondamentale. Con questo non si vuole però sminuire il ruolo che le nuove tecnologie hanno nella società attuale, ma solo sottolineare come non vi siano attualmente i presupposti giuridici per far rientrare la connessione al *web* nella categoria appena menzionata. Si può però correttamente affermare che la navigazione nel *cyberspace* è un diritto sociale, data la sua importanza più volte menzionata nel corso della presente trattazione. Coloro che non sono in grado di connettersi al *web* risultano infatti "esclusi" da molte opportunità di integrazione nella propria comunità. La normativa Ue ha preso coscienza di questo attraverso la categoria del "servizio universale": lo Stato deve quindi impegnarsi attivamente per garantire ai propri cittadini i mezzi, sia tecnologici che culturali, per poter navigare in Internet

La rete dovrebbe inoltre rispecchiare i caratteri di neutralità per permettere agli utenti di godere effettivamente dei suoi benefici. La classificazione come "servizio universale" perderebbe infatti di significato qualora il cittadino non avesse le disponibilità economiche per usufruire dei contenuti eventualmente disponibili a pagamento in rete. Questo studio auspica quindi, pur nei limiti delle disponibilità in termini di risorse di ogni Stato, che l'Unione europea e la comunità internazionale proseguano nella strada verso uno spazio cibernetico liberamente accessibile e neutrale.

Capitolo 3

Il diritto alla libera espressione nell'era cibernetica e gli strumenti per tutelare la libertà di parola nel web

Sommario: Introduzione - 1. Dai media tradizionali al web: l'evoluzione del mercato dell'informazione e le sue conseguenze giuridiche. - 1.1. Il pluralismo delle fonti di informazione: visioni critiche a confronto. – 1.2. Internet e la nuova struttura della comunicazione nell'era digitale. - 2. L'evoluzione filosofico-normativa del diritto alla libera espressione: dall'Antica Grecia al riconoscimento nei trattati internazionali. - 2.1. Il diritto alla libera espressione nella Dichiarazione Universale dei Diritti dell'Uomo. - 2.1.1. Il lavoro del Consiglio per i Diritti Umani e dello Special Rapporteur sulla libertà di espressione. - 2.2. Il riconoscimento nel Patto Internazionale sui Diritti Civili e Politici della libertà di espressione indipendentemente dal mezzo di comunicazione utilizzato. - 2.3. La tutela del diritto alla libera espressione negli accordi regionali. - 2.3.1. Il diritto alla libera espressione nell'azione del Consiglio di Europa e il suo riconoscimento nel diritto europeo primario. - 2.3.2. La Carta di Parigi a tutela della libertà di espressione. - 2.3.3. La difesa della libertà di espressione nel continente africano: la Carta africana dei diritti dell'uomo e dei popoli. - 2.3.4. Gli accordi regionali nel continente americano a difesa della libertà di espressione. - 3. La responsabilità degli Internet Service Provider nella tutela del diritto alla libera espressione nella giurisprudenza della Corte di giustizia dell'Unione europea. - 4. I limiti della libera espressione nel contesto cibernetico secondo la giurisprudenza della Corte europea dei diritti umani e della Corte di giustizia dell'Unione europea. - 5. Gli effetti collaterali della comunicazione nell'epoca digitale: il fenomeno della filter bubble e l'imperativo dello sharing. - 6. La diffusione delle fake news. I possibili rimedi giuridici all'inquinamento del public discourse. - 6.1. Il report della Commissione europea sulle fake news. - 7. Riflessioni conclusive.

Introduzione

"*L'idea di alcune persone della libertà di parola è che sono liberi di dire quello che vogliono, ma se qualcuno gli risponde, lo considerano oltraggio"* (W.Churchill)[246].

Le parole dell'ex primo ministro inglese sono un chiaro esempio della dimensione antagonista del diritto alla libera espressione, volto a tutelare le idee espressione di una parte minoritaria della collettività. Risulta di per sé evidente che il pensiero dell'élite dominante non ha bisogno di alcuna protezione.

Il mantenimento dell'ordine democratico è garantito dal dibattito politico quale strumento di una proficua crescita sociale; non è un caso che qualsiasi dittatura o regime autoritario succedutosi nel corso dei secoli ha visto la più grande minaccia al proprio successo nel libero pensiero e nella diffusione delle idee.

[246] Frase pronunciata da W.CHURCHILL durante un discorso al Parlamento inglese in data 13 ottobre 1943.

L'importanza del libero pensiero per la tenuta delle moderne democrazie è quanto mai attuale nella moderna epoca digitale. I *social media* come Facebook o Twitter sono piattaforme digitali divenute fondamentali per il dialogo politico e per la formazione di una coscienza pubblica.

Il diritto alla libera espressione è strettamente collegato al diritto all'informazione: solamente una persona adeguatamente informata può esprimere la propria opinione in maniera efficace e con cognizione di causa. Alla luce di ciò, giova sottolineare che gli stessi *social* sono diventati una delle fonti primarie di informazione[247]; il 62% dei cittadini americani dichiara di utilizzare le piattaforme sociali per leggere le ultime notizie e il 18% di loro afferma di farlo frequentemente. La percentuale cresce nella fascia di età tra i 18 e i 29 anni, raggiungendo la cifra dell'81%. Nell'epoca attuale, portali informatici gestiti da società multinazionali private svolgono funzioni fondamentali per l'intera collettività, garantendo la circolazione delle informazioni e dando altresì ai propri utenti uno spazio dove esprimere la propria opinione. Il possibile corto circuito politico-normativo è presto evidente: grandi compagnie imprenditoriali, che rispondono esclusivamente alla logica del profitto economico e che non devono rispondere in alcun modo ai pubblici poteri, hanno il potere pressoché insindacabile di censurare determinate idee, impedendone la diffusione sui propri portali e condannandole quindi all'oblio.

Le disposizioni normative, sia a livello statale che internazionale, poste a tutela del diritto alla libera espressione rischiano di rivelarsi ora inadeguate, poiché sono state ideate e predisposte pensando ai tradizionali sistemi di comunicazione. Fino a pochi anni fa, le principali fonti di informazioni erano le Tv e la carta stampata. Le notizie seguivano un percorso verticale, fluendo dai giornalisti ai lettori/spettatori che erano i destinatari finali di questo percorso ed erano relegati a un mero ruolo passivo di fruitori. Le reti digitali hanno completamente rivoluzionato questa prospettiva, formando degli snodi di comunicazione verticali: ogni utente cibernetico, attraverso l'utilizzo del proprio *device* elettronico, può far sentire la propria voce via *web*, rivestendo nel medesimo tempo sia il ruolo di comunicatore che di fruitore delle notizie. In questa situazione, il ruolo dei *mass media* tradizionali viene drasticamente ridimensionato, a discapito anche del loro prestigio.

[247] P.COSTA, *Motori di ricerca e social media: i nuovi filtri nell'ecosistema dell'informazione on-line e il potere occulto degli algoritmi,* in (a cura di) G.AVANZINI, G.MATUCCI, *L'informazione e le sue regole. Libertà, pluralismo e trasparenza*, Napoli, 2016, pp.257.

L'utilizzo delle nuove tecnologie di comunicazione ha indubbi lati positivi, poiché rende il diritto alla libera espressione all'effettiva portata di ogni persona, favorendo inoltre la rapida circolazione delle informazioni. Non devono però essere trascurati i possibili lati negativi, in particolar modo riguardanti il fenomeno delle cd. *fake news*.

I grandi network delle comunicazioni, come giornali e radiotelevisioni, garantivano l'attendibilità delle notizie diffuse; questo non è più possibile nel contesto cibernetico. Qualsiasi utente può infatti diffondere consapevolmente notizie artefatte e intenzionalmente false, con l'intento di inquinare il *public discourse* influenzando così la formazione dell'opinione pubblica. La struttura stessa dei *social media,* basata sull'imperativo della condivisione dei contenuti, il cd. *sharing*, si dimostra l'ambiente ideale per far proliferare e diffondere queste "false notizie". Il grande numero di utenti connessi alle piattaforme sociali rende pressoché impossibile un controllo preventivo sull'attendibilità delle notizie diffuse attraverso il *web*; inoltre, qualora anche tale controllo fosse astrattamente possibile, si solleverebbero pressanti interrogativi su eventuali abusi e limitazioni alla libera espressione degli utenti stessi.

Simili problematiche non erano contemplate al momento dell'emanazione delle norme a tutela del diritto alla libertà di pensiero; è perciò necessario riflettere se tale principio debba essere riadattato alle esigenze del contesto cibernetico.

Per rispondere a questa esigenza, il presente studio prende le mosse da una completa analisi dei cambiamenti che le nuove tecnologie digitali hanno apportato al tradizionale sistema di comunicazioni. Si passa poi a studiare l'oggetto principale dell'articolo, ossia il diritto alla libera espressione, per comprendere come questo sia stato riconosciuto a livello europeo e internazionale nel corso degli anni. La terza parte dello studio vuole riflettere sulle risposte normative e giurisprudenziali che, nel corso degli anni, sono state date ai fenomeni appena menzionati delle *fake news.* Solo al termine di questa analisi sarà possibile capire le caratteristiche fondamentali del diritto alla libera espressione nel contesto cibernetico e le modalità più funzionali per tutelare tale principio adeguatamente.

1. *Dai media tradizionali al web: l'evoluzione del mercato dell'informazione e le sue conseguenze giuridiche*

Internet e le nuove tecnologie digitali hanno rivoluzionato in breve tempo il tradizionale modo di comunicare; ogni utente cibernetico è ora in grado di entrare in

contatto attraverso pochi *click*, e ad un prezzo irrisorio, con persone che vivono all'altro capo del pianeta. Una società costantemente connessa e informatizzata, dove flussi di informazioni viaggiano a velocità istantanea nello spazio cibernetico, era francamente impensabile fino a pochi anni fa.

Un così radicale cambiamento ha conseguenze inevitabili anche sulla concezione della libertà di espressione e sulla sua effettiva applicazione nell'attuale contesto digitale. Il diritto alla libertà di parola è un caposaldo fondamentale del costituzionalismo moderno, nonché un elemento imprescindibile dell'ordinamento di qualsiasi Stato che si vuole definire democratico[248]. L'attiva partecipazione alla vita politica della propria comunità può essere assicurata solamente in una società caratterizzata da tale diritto, dove ogni persona si sente libera di esprimere la propria opinione senza dover temere alcuna ritorsione. L'art.XI della Dichiarazione dei Diritti dell'Uomo e del Cittadino[249] proclamò la libertà di espressione come uno dei diritti più preziosi per l'essere umano. Ogni persona avrebbe dovuto avere la possibilità di scambiare informazioni senza dover temere ingerenza alcuna in tale ambito. Questa libertà si presenta quindi sotto un duplice aspetto, sia positivo che negativo: da una parte si riconosce il diritto a tutti i cittadini di esprimere liberamente la propria opinione, dall'altra si vieta allo Stato e ai pubblici poteri di agire in maniera tale da limitare od ostacolare l'esercizio del summenzionato diritto.

L'importanza delle parole della Dichiarazione dei Diritti dell'Uomo e del Cittadino è testimoniata dall'enorme influenza che hanno avuto nella scrittura e nella proclamazione dei testi costituzionali successivi in tutta la cultura giuridica occidentale; la protezione normativa garantita al diritto alla libera espressione si basa infatti ancora oggi sui medesimi fondamenti stabiliti nell'ormai lontano 1789, nonostante gli enormi cambiamenti che sono avvenuti nel mondo della comunicazione e a cui prima si accennava[250].

Prima dell'avvento di Internet, il mercato dell'informazione era tradizionalmente basato in maniera pressoché esclusiva sull'operato dei grandi gruppi editoriali; erano gli unici in grado di raccogliere gli ingenti capitali necessari per costruire gli stabilimenti tipografici dove stampare i giornali. Esistevano quindi delle insormontabili barriere

[248] J.B.MIR, M.BASSINI, *Freedom of expression in the Internet. Main trends of the case law of the European Court of Human Rights*, in (a cura di) O.POLLICINO, G.ROMEO, New York, NY, 2016, pp.71-94.
[249] La Dichiarazione dei Diritti dell'Uomo e del Cittadino, proclamata il 26 agosto 1789, racchiude un elenco di diritti fondamentali riconosciuti all'essere umano in quanto tale. Il testo è consultabile al seguente link http://www.dircost.unito.it/cs/docs/francia1789.htm (consultato il 2 settembre 2019).
[250] J.B.MIR, M.BASSINI, *op.cit.*

all'ingresso che limitavano effettivamente l'esercizio della libertà di informazione solo a coloro che disponevano delle necessarie risorse economiche per entrare in tale mercato[251]. Ad un formale riconoscimento globale del diritto alla libertà di parola da parte dei testi costituzionali non corrispondeva perciò un effettivo esercizio di tale diritto per tutti i cittadini.

La circolazione delle informazioni secondo questo modello aveva un'importante influenza anche sulla formazione del pensiero politico: gli editori, privilegiando la comunicazione di una notizia rispetto ad un'altra, contribuivano a orientare il pensiero dell'opinione pubblica verso una particolare direzione rispetto ad un'altra. Il diritto alla libera espressione è infatti legato a doppio filo al diritto all'informazione: sono stati infatti elaborati in un'epoca in cui una ricca borghesia rivestiva il ruolo di classe sociale dominante, con le capacità economiche necessarie per indirizzare la vita politica della collettività[252]. Solamente le persone istruite potevano infatti leggere i giornali e i libri, mantenendosi così informati sugli ultimi avvenimenti. D'altronde, la libera espressione del pensiero può avvenire solo dopo la formazione del pensiero stesso; solamente coloro che si erano documentati potevano esprimere la loro opinione con un'effettiva cognizione di causa.

L'avvento delle radio e delle televisioni ha portato a una sorta di "massificazione" dell'informazione[253]; chiunque sia in grado di disporre di un apparecchio radiotelevisivo può infatti ricevere costantemente notizie attraverso i programmi Tv e i telegiornali. Sono però i *network* televisivi a decidere quali informazioni condividere e di quali privilegiare la diffusione; poche e potenti "voci" possono perciò formare e orientare il pensiero di un enorme numero di persone.

1.1. Il pluralismo delle fonti di informazione: visioni critiche a confronto

Considerato ciò, diventa necessario garantire il pluralismo delle fonti di informazione; la competizione tra gli editori dovrebbe auspicabilmente impedire la formazione di monopoli e quindi di un "pensiero unico". Lo sforzo del legislatore a tal

[251] G.PITRUZZELLA, *La libertà di informazione nell'era di Internet*, in *Rivista di diritto dei media*, n.1, 2018, pp.1-28.
[252] J.B.MIR, M.BASSINI, *op.cit.*
[253] V.ZENO-ZENCOVICH, *Freedom of expression. A critical and comparative analysis*, New York, 2008, pp.23-40.

proposito deve essere perciò indirizzato a formulare norme in materia di *antitrust*, per garantire un mercato dell'informazione concorrenziale[254].

L'intento di tali misure è di garantire che nessuna voce rimanga inascoltata, neppure quella che si oppone al pensiero dominante; la presenza sul mercato di numerosi gruppi editoriali potrebbe assicurare questo risultato[255]. Incaricare i *mass media* di diffondere anche le voci minoritarie e potenzialmente inascoltate fa sì che i grandi *network* dell'informazione non rivestano più un ruolo esclusivamente economico-industriale, ma anche una funzione pubblica[256]. Se il ruolo dei *media* fosse solo quello di offrire il proprio prodotto in un'ottica meramente commerciale, lo Stato non dovrebbe intervenire a regolamentare il mercato dell'informazione, lasciando libero il pubblico di decidere quale telegiornale vedere e quale giornale comprare. L'azione pubblica nel settore dell'informazione è invece giustificata dal fatto che si ritiene tale ambito fondamentale per la stabilità democratica dello Stato stesso.

Le modalità attraverso le quali garantire un effettivo pluralismo delle fonti di informazione sono state per molti anni al centro del dibattito, suscitando posizioni spesso contrapposte[257]. Le maggiori critiche rivolte all'approccio ora menzionato sono ben esemplificate da un semplice paradosso: Per gli oppositori di tale visione[258] l'idea di voler tutelare la varietà delle idee attraverso la presenza di numerose compagnie di *mass media* avrebbe la stessa fondatezza di voler salvaguardare l'ambiente attraverso la creazione di sempre più industrie di detergenti. Risulta infatti complesso dimostrare una qualsiasi voglia relazione causa-effetto tra il numero dei *network* presenti sul mercato dell'informazione e la qualità dei prodotti finali offerti. Secondo tale corrente di pensiero, il mercato concorrenziale non significa automaticamente una varietà dei contenuti prodotti; non è infatti raro che i giornali, per non diminuire il numero di copie vendute, si trovino a dover riproporre con un taglio differente le medesime notizie già pubblicate, e lo stesso vale per i telegiornali[259].

---

[254] G.PITRUZZELLA, *op.cit.*

[255] V.PORTER, S.HASSELBACH, *Politics and the Market-place. The regulation of German Broadcasting*, Londra, 1991, pp.4 ss.

[256] T.GIBBONS, *Regulating the media,* Londra, 1998, pp.48 ss.

[257] V.ZENO-ZENCOVICH, *op.cit.*

[258] D.MCQUAIL, *Media performance: mass comunication and the public interest*, Londra, 1992, pp.124 ss.; D.GOMERY, *Interpreting media ownership*, in (a cura di) B.M.COMPAINE, D.GOMERY, *Who owns the media? Competition and concentration in the mass media industry*, Londra, 2000, pp.529 ss.

[259] D.MCQUAIL, K.SIUNE, *Media policy. Convergence, concentration and commerce*, Londra, 1998, pp.56 ss.

Non mancano certo modalità alternative per diffondere le idee minoritarie e i pensieri differenti rispetto alle ideologie dominanti; si pensi a misure per facilitarne la diffusione come sussidi economici o spazi di comunicazioni riservati sui giornali o sui canali televisivi[260]. Qualora una di queste idee risultasse interessante e una potenziale fonte di profitto economico, qualcuno potrebbe decidere di investirci e darle quindi un risalto ancora maggiore; la strategia da perseguire sarebbe quindi quella di una graduale differenziazione tra le informazioni messe sul mercato invece di una loro standardizzazione omogenea[261]. Non viene ravvisato alcun vantaggio economico nel voler diffondere in maniera forzata idee che il mercato delle informazioni non reputa profittevoli, a discapito di pensieri che invece riceverebbero ben altra accoglienza[262].

Un pluralismo delle fonti di informazione imposto dalla legge potrebbe avere il risultato paradossale di limitare il diritto alla libera espressione di quei soggetti che dovrebbero tacere per dare spazio ad altre idee, anche se queste non rispecchiano che una sparuta minoranza della società[263]. Occorre infatti chiedersi quali pensieri meritino una maggiore diffusione a discapito di altri e secondo quali criteri dovrebbe essere compiuta tale scelta. Sembra quantomeno contradditorio che il compito di scegliere spetti allo Stato: perché dovrebbero essere i pubblici poteri a indicare quali pensieri minoritari, atti a funzionare da contraltare all'ideologia dominante, privilegiare rispetto ad altre idee? La diversità dovrebbe essere un bene strumentale e non il fine stesso della politica statale nel campo dell'informazione[264].

D'altro canto, lasciare spazio all'autoregolamentazione del mercato in un settore così delicato da un punto di vista sociale e democratico come quello dei *mass media* potrebbe essere una scelta avventata. La formazione di una posizione di monopolio in capo a potenti *network*, come si diceva poc'anzi, potrebbe infatti causare delle distorsioni nella formazione del pensiero politico dell'opinione pubblica. Le idee che non riscontrano il gradimento dei grandi editori finirebbero presto dimenticate e inascoltate.

---

[260] O.M.FISS, *Why the State?*, in (a cura di) J.LICHTENBERG, *Democracy and the media*, Cambridge, 1990, pp.146 ss.
[261] E.NOAM, *Two cheers for the commodification of information*, in (a cura di) N.ELKIN KOREN, N.W.NETANEL, *The commodification of information*, L'Aja, 2002, pp.48 ss.
[262] T.GIBBONS, op.cit., p.33; D.KELLEY, R.DONWAY, *Liberalism and free spech*, in J.LICHTENBERG, op.cit., pp.81.
[263] La Commissione europea si è espressa su questa linea di pensiero attraverso il *Green Paper on pluralism and media concentration* (COM (92) 480 final). La posizione della Commissione è stata accolta da molte critiche: a tal proposito si veda R.MAZZA, *Diffusione televisiva e disciplina comunitaria della concorrenza*, Torino, 2002, p.48.
[264] D.KELLEY, R.DONWAY, *op.cit.*, pp. 88.

In conclusione, il "mercato delle idee" non può essere trattato come un qualsiasi altro settore economico, data la sua importanza e la sua funzione sociale; l'intervento statale volto a tutelare le idee minoritarie e le posizioni che non rispecchiano quelle dominanti nell'opinione pubblica appare necessario per garantire la tenuta dell'ordinamento democratico. L'azione dei pubblici poteri deve però seguire linee ben precise, non andando a influenzare più del necessario la libera circolazione di idee all'interno della collettività, imponendo arbitrariamente un pensiero al posto di un altro. Occorre perciò individuare dei metodi che permettano a ogni persona di poter esprimere la propria opinione e di far sì che questa venga diffusa e ascoltata senza la necessità degli enormi investimenti necessari per la pubblicazione di un giornale o per la ripresa televisiva di un telegiornale. In poche parole, occorre uno strumento che permetta a qualsiasi individuo di diventare un produttore di informazioni.

1.2. Internet e la nuova struttura della comunicazione nell'era digitale

Internet e le reti digitali possono essere la risposta a questo crescente bisogno. La crescente diffusione del *world wide web* ha avuto innegabili conseguenze sulle tradizionali modalità di comunicazione e sulla comune struttura del mercato dei *mass media* come. Nella società odierna è infatti sufficiente avere un qualsiasi *device* elettronico, come uno *smartphone* o un *laptop*, per avere la disponibilità di una connessione cibernetica e poter quindi condividere il proprio pensiero con gli altri utenti del mondo virtuale.

Questo favorisce la progressiva introduzione di un modello di comunicazione basato sul *peer-to-peer*[265], secondo il quale un numero elevato di individui produce informazioni e cultura in maniera autonoma, senza alcuna coordinazione o influenza da parte di capitali e/o compagnie editoriali. Il tradizionale assetto verticale della circolazione delle notizie, dal giornale al lettore che si limitava al ruolo di mero fruitore passivo, viene gradualmente messo in discussione in favore di snodi comunicativi orizzontali. Inizia a perdere di significato la distinzione tra *senders* e *receivers*, tra coloro che inviano le notizie e quelli che le ricevono[266]; l'utente cibernetico può infatti rivestire entrambi i ruoli allo stesso tempo.

---

[265] Y.BENKLER, *The wealth of networks: how social production transforms markets and freedom*, New Haven CT, 2006, pp.31 ss.
[266] J.B.MIR, M.BASSINI, *op.cit.*.

A tal proposto si può parlare di *network information economy*[267], i cui tratti principali possono essere così riassunti: a) una progressiva decentralizzazione delle fonti di informazioni. Ogni utente della rete cibernetica è infatti un potenziale produttore di notizie e pensieri, dotato della "cassa di risonanza" che è il *web*; b) la disponibilità a prezzi relativamente bassi dei *device* elettronici necessari alla connessione Internet fa sì che la possibilità di comunicare le proprie idee sia alla portata di tutti; c) la diffusione globale delle reti digitali ha reso possibile comunicare in tempo reale con ogni angolo del pianeta.

Si è parlato anche di *mass self-communication* per definire sistemi di comunicazione organizzati su base orizzontale portati avanti su base individuale da numerosi utenti che condividono contenuti di carattere multimediale[268].

Il nuovo scenario svelato dal mondo cibernetico ha cambiato radicalmente la funzione dei *mass media* tradizionali[269] che, grazie all'avvento di Internet, hanno perso il loro ruolo di fonte primaria e privilegiata di informazioni[270]. Le reti digitali, riducendo il numero di intermediari nella circolazione delle notizie, ne riducono l'importanza e anche il loro costo; non sono più strettamente necessari gli investimenti volti alla pubblicazione di giornali e riviste[271].

Non bisogna però cadere nell'errore di ritrarre il mondo cibernetico come un ambiente dove ogni utente ha le stesse potenzialità di qualsiasi altro; nuovi importanti attori, soprattutto di natura privata, si sono affermati come gestori e custodi dei flussi di informazione che navigano per il *world wide web*.

Internet rende liberamente disponibili ai propri utenti enormi quantitativi di dati e notizie; può risultare assai complicato per un semplice individuo districarsi in questo *mare magnum* di informazioni. Non può più limitarsi ad essere mero fruitore di ciò che gli viene trasmesso da giornali e televisioni, ma deve impegnarsi in prima persona nel ricercare le notizie che lo interessano[272].

Assume una rinnovata importanza il ruolo dei soggetti capaci di organizzare questa massa di dati in maniera intellegibile per ogni utente, facilitando inoltre il collegamento tra coloro che sono in possesso dell'informazioni e quelli che invece

---

[267] Y.BENKLER, *op.cit.*
[268] M.CASTELLS, *Communication power*, Oxford, 2009, pp.18 ss.
[269] B.M.COMPAINE, *Distinguishing between concentration and competition*, in (a cura di) B.M.COMPAINE, D.GOMERY, *op.cit.*, pp.538 ss.
[270] M.E.KATSCH, *The electronic media and the transformation of law*, New York, 1989, pp.116 ss.
[271] B. MCNAIR, *Journalism and democracy. An evaluation of the political public sphere*, Londra, 2000, pp.178 ss.
[272] V.ZENO-ZENCOVICH, *op.cit.*, pp.101.

vogliono riceverla[273]; sono i *gatekeepers*, i portieri dello spazio cibernetico[274]. Un mercato delle informazioni apparentemente libero e senza restrizioni è invece governato da un ristretto numero di compagnie informatiche che lo gestiscono secondo i loro interessi. Aziende come Google, Facebook, Apple agiscono da aggregatori di contenuti, decidendo quali informazioni privilegiare in termini di visibilità nei risultati delle ricerche *on-line* effettuate dagli utenti.

Si riscontra una sorta di ambiguità di fondo nella natura dello spazio cibernetico: a un'apertura e decentralizzazione senza precedenti corrisponde però una concentrazione del potere di gestione delle informazioni in mano a poche grandi multinazionali private che non devono rispondere del proprio operato a nessuna collettività sociale, se non a quella dei propri azionisti[275].

Non si deve perciò trascurare l'eventualità che si riproponga, seppur con caratteristiche diverse, il rischio di un mancato rispetto del pluralismo delle fonti di informazione, con un conseguente detrimento della formazione di un pensiero politico libero e indipendente nella collettività. Rispetto a quanto accadeva nell'epoca in cui gli unici attori presenti nel settore dei *mass media* erano i grandi *network*, ora occorre però considerare che anche i singoli individui possono diventare produttori di informazioni. Molti dei contenuti generati dagli utenti vengono immessi e condivisi non su siti Internet privati, ma su piattaforme multimediali gestite dalle grandi compagnie a cui prima si faceva riferimento. Si pensi a portali informatici di fama mondiale come Youtube o Instagram, attraverso i quali vengono condivisi quotidianamente milioni di foto e video. I gestori di queste piattaforme sono investiti di un potere potenzialmente enorme[276], perché hanno l'ultima parola su quali contenuti possono essere resi disponibili in rete e quali invece devono rimanere nascosti nei meandri del *world wide web*; si potrebbe dire che svolgono il ruolo di "censori" del mondo cibernetico. Una simile funzione solleva però delle importanti questioni, sia di segno etico che più strettamente giuridico. Dei soggetti privati, che rispondono quindi unicamente alle logiche del mercato e non a motivazioni di carattere sociale o politico, devono essere in grado di decidere quali informazioni possono essere trasmesse nel *cyberspace*? Questo potere deve rimanere in

[273] G.PITRUZZELLA, *op.cit.*
[274] E.B.LAIDLAW, *Regulating speech in cyberspace*, Cambridge, 2015, pp.44 ss.
[275] G.PITRUZZELLA, *op.cit.*
[276] J.B.MIR, M.BASSINI, *op.cit.*

mani private senza alcuna supervisione statale o è invece più ragionevole passare a un controllo pubblico? In caso di risposta affermativa, attraverso quali modalità?

La risposta a queste domande può avere importanti conseguenze sull'effettiva natura del diritto alla libera espressione e sul suo futuro sviluppo nel campo cibernetico. Come si accennava poc'anzi, Internet ha rivoluzionato il modo di comunicare, influenzando radicalmente anche il diritto al libero pensiero riscoprendone la sua dimensione più strettamente individuale e personalistica. Prima dell'avvento delle reti digitali, l'effettivo utilizzo della libertà di parola era limitato a coloro che avevano a disposizione i mezzi per far sentire la propria voce: si pensi ai proprietari dei grandi giornali o dei *network* televisivi. Le altre persone potevano certamente avere la possibilità di esprimere la propria opinione, ma non avevano gli strumenti per far sentire la propria voce.

Pur rimanendo i tradizionali *mass media* ancora dominanti, i singoli individui hanno ora la possibilità di diffondere le proprie idee attraverso il *world wide web* senza dover ricorrere ai mezzi utilizzati dalle grandi compagnie del mercato dell'informazione. La velocità della connessione, la possibilità di condividere contenuti multimediali, la relativa economicità e semplicità dei *device* necessari alla navigazione in rete sono tutti elementi che contribuiscono a rendere l'accesso e l'utilizzo di Internet alla portata di buona parte della popolazione mondiale.

Il funzionamento dello spazio cibernetico si basa sulla digitalizzazione dei messaggi[277] e sulla trasmissione di tali dati. Qualsiasi informazione, che si tratti di audio, video o testo, viene digitalizzata una volta immessa nella rete e i costi della sua condivisione sono uguali in qualsiasi parte del mondo. L'utente cibernetico è quindi libero di "scaricare" questi dati dal *web* senza alcuna restrizione data dalla sua localizzazione geografica e dal luogo di connessione.

Il diritto alla libera espressione può quindi essere inteso anche come libertà di condivisione di dati o, più propriamente, *freedom to disseminate data*[278]. La nascita di un nuovo diritto, o perlomeno la sua evoluzione, richiede necessariamente una sua definizione adatta al contesto in cui deve applicarsi, ossia quello cibernetico, in relazione alle sue caratteristiche e ai suoi obbiettivi. Questo è un passo fondamentale per comprendere se le tradizionali categorie giuridiche possono dirsi ancora adatte a tutelare efficacemente il libero pensiero nel *cyberspace*.

[277] V.ZENO-ZENCOVICH, *op.cit.*, pp.102.
[278] V.ZENO-ZENCOVICH, *ibidem.*

Prima di poter risolvere questo quesito, occorre però riflettere in maniera approfondita sul contenuto stesso del diritto alla libera espressione, per comprenderne appieno la natura e per capirne le esigenze di tutela nell'epoca della società digitale.

2. *L'evoluzione filosofico-normativa del diritto alla libera espressione: dall'Antica Grecia al riconoscimento nei trattati internazionali*

Il diritto alla libera espressione ha radici antiche, che si perdono nella notte dei tempi della civiltà. Una prima elaborazione filosofica di questo principio si ha nell'Antica Grecia[279]; la libertà intellettuale propugnata dal pensiero razionalista di Democrito ed Eraclito potrebbe essere infatti intesa come diretta antesignana del libero pensiero. Socrate, nella sua *Apologia,* affermava il valore fondamentale della pubblica discussione per la tenuta della *polis*.

Una prima definizione del diritto alla libertà di parola si ha con lo scritto di Milton del 1664 *Aeropagitica: discorso per la libertà di stampa*. Il pensatore inglese, criticando un provvedimento del Parlamento britannico che imponeva un sistema di licenze e permessi amministrativi alle stamperie e agli editori, affermava il diritto innato dell'essere umano a seguire il proprio intelletto attraverso la circolazione delle idee, riconoscendo inoltre il valore della discussione e del dibattito come strumenti per far progredire la società.

Come accennato precedentemente, in un'epoca risalente il diritto alla libera espressione era esclusivo appannaggio delle classi dominanti che avevano a disposizione i mezzi economici per poter far sentire la loro opinione. Questa realtà dei fatti era testimoniata dal *Bill of Rights*[280] inglese del 1689 che riconosceva la libertà di parola esclusivamente a membri del Parlamento, limitandone peraltro l'esercizio alle sole prerogative delle funzioni parlamentari.

Il *Bill of Rights* della Virginia del 1776, frutto dell'indipendenza delle colonie britanniche oltreoceano, compiva un importante passo in avanti affermando, alla sez.12, che *la libertà di stampa è uno dei più grandi baluardi della libertà e non può mai essere limitata da governi dispotici*. Risulta evidente il legame, che andrà rafforzandosi sempre

[279] G.SARTORI, *Elementi di teoria politica,* Bologna, 1995, pp.174; J.BURY BAGNELL, *Storia della libertà di pensiero*, Milano, 1962, pp.41 ss.
[280] Una versione tradotta del *Bill of Rights* inglese può essere consultata su G.DALL'OLIO, *Storia moderna*, Roma, 2004, pp.222-223.

di più nelle epoche successive, tra la tecnologia dei mezzi di comunicazione e la libertà di espressione. Si ravvisa inoltre una profonda consapevolezza dello stretto rapporto tra informazione e formazione della coscienza pubblica; l'utilizzo della stampa permetteva infatti la diffusione di libri e giornali che potevano orientare l'opinione politica della collettività, anche in maniera contraria rispetto all'ideologia dominante.

Il diritto alla libertà di parola veniva riconosciuto su tutto il territorio statunitense nel 1791, con l'approvazione del Primo Emendamento alla Costituzione americana[281], così come elaborato dal *Bill of Rights* statunitense del 1789. I costituenti statunitensi intuivano che il diritto alla libera espressione e alla libertà di informazione funzionava da limite a possibili abusi governativi; un popolo informato e cosciente dei propri diritti non poteva essere infatti soverchiato facilmente dai pubblici poteri.

L'influenza della Carta dei Diritti americana è evidente nella Dichiarazione dei Diritti dell'Uomo e del Cittadino, a cui si accennava poc'anzi. Le caratteristiche del diritto alla libera espressione fissate in Francia nel 1789 si ritrovano anche nel costituzionalismo moderno; il riconoscimento del suo carattere fondamentale e insito all'essere umano, ma anche il potere dello Stato di fissarne i limiti per ottenere un efficace bilanciamento con altri diritti parimenti meritevoli di tutela[282].

Il libero pensiero diventa dei risultati principali della cultura illuminista; l'essere umano acquisisce importanza in quanto tale e così anche la sua parola e le sue idee, che meritano perciò un'adeguata tutela.

Il diritto internazionale ha gradualmente riconosciuto questa concezione, fino ad arrivare a sancire l'intangibilità del diritto alla libera espressione nel corso del XX secolo. I due conflitti mondiali, scatenati da regimi dittatoriali e repressivi, hanno evidenziato ancora di più il ruolo fondamentale della libera espressione nel mantenimento di uno stabile ordine democratico. Nonostante questa convinzione, gli strumenti pattizi a difesa dei diritti umani, e in particolar modo della libertà di pensiero, non sono esenti da deroghe e limitazioni[283]. Si tratta di un tema particolarmente delicato per la comunità internazionale, considerate le differenti influenze culturali e sociali che caratterizzano il dibattito politico nei differenti Paesi. Un'idea ritenuta tollerabile, o addirittura

[281] Una trascrizione ufficiale del *Bill of Rights* statunitense è disponibile al seguente link: https://www.archives.gov/founding-docs/bill-of-rights-transcript (consultato il 10 settembre 2019).
[282] M.OROFINO, *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione*, Torino, 2014, pp.37 ss.
[283] P.E.ROZO SORDINI, *La libertà di espressione nell'era digitale. Disciplina internazionale e problematiche, ISPI Working Paper*, n.52, ottobre 2013, pp.7.

condivisibile, in una determinata nazione, può essere infatti considerata oltraggiosa in un altro specifico Stato. Partendo da questi presupposti, si comprende come sia difficilmente raggiungibile un riconoscimento vincolante a livello globale della libertà di espressione, per non parlare di una sua effettiva regolamentazione.

2.1. *Il diritto alla libera espressione nella Dichiarazione Universale dei Diritti dell'Uomo*

La Dichiarazione Universale dei Diritti dell'Uomo[284] (d'ora in poi anche DUDU) approvata in seno alle Nazioni Unite nel 1948 ha rappresentato forse il passo più importante per affermare il valore della libertà di espressione nel diritto internazionale. L'art. 12 di tale atto afferma che nessuna persona deve subire alcuna ingerenza nella propria vita privata e famigliare. Deve rimanere inviolata anche la corrispondenza inviata e ricevuta. La protezione si estende alla sfera dell'onore e della reputazione, che non deve subire ingiusti attacchi sia dai pubblici poteri che da soggetti privati.

L'articolo in questione solleva diversi spunti di riflessione, valevoli anche per il contesto digitale, che non devono essere trascurati. Risulta evidente il legame tra diritto alla privacy e libertà di espressione: una persona può essere libera di esprimere il proprio pensiero solamente nel caso in cui la sua sfera privata risulti non intaccata e inviolabile. Nel caso contrario, potrebbe infatti temere ritorsioni nei propri confronti o verso i propri affetti, decidendo quindi di tacere e di non esercitare il proprio diritto alla libertà di parola. Riveste particolare importanza anche il riferimento all'inviolabilità della corrispondenza; si può riconoscere in questa disposizione il passaggio da una concezione della privacy intesa come "diritto ad essere lasciati soli", così come formulata nel celebre articolo[285] di Warren e Brandeis del 1890 ad un diritto a far circolare le informazioni. La riservatezza non si limita più alla sfera privata concreta e materiale, ma si estende anche ai dati fatti circolare.

Proseguendo nell'analisi di quanto statuito dalla Dichiarazione Universale dei Diritti dell'Uomo, si riscontra la categorica affermazione dell'art.19, secondo il quale ogni essere umano vanta il diritto alla libertà di opinione e di espressione, che include la prerogativa di esternare le proprie convinzioni senza timore di ingerenza alcuna, così

[284] Il testo ufficiale della Dichiarazione Universale dei Diritti dell'Uomo, approvato dall'Assemblea Generale delle Nazioni Unite il 10 dicembre 1948, è disponibile al seguente link https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/itn.pdf (consultato il 16 settembre 2019).
[285] S.WARREN, L.D.BRANDEIS, *The right to privacy,* in *Harvard Law Review,* n.4, 1890, pp.193 ss.

come quella di cercare, diffondere e ricevere informazioni attraverso qualsiasi mezzo di comunicazione senza dover tenere conto di confini o barriere. Nelle parole della DUDU risulta evidente lo stretto legame tra libertà di espressione e diritto all'informazione; solamente la persona informata può far sentire la propria voce con un'effettiva cognizione di causa.

L'articolo 19 appena menzionato può trovare una valida applicazione anche nel mondo cibernetico[286]. Il testo della norma fa riferimento alla possibilità di "ricevere" e "diffondere" informazioni (*receive* e *impart* nella formulazione originale in lingua inglese); l'elenco dei comportamenti permessi descrive perfettamente la navigazione *on-line* di qualsiasi utente cibernetico. D'altronde, una qualsiasi connessione Internet non si risolve in altro che in una continua condivisione di dati con i restanti membri della rete informatica.

La formulazione dell'articolo 19 lascia presupporre che i suoi estensori fossero consapevoli delle possibilità di sviluppo dei mezzi di comunicazione e volessero far sì che il loro lavoro non diventasse presto obsoleto, ma fosse invece adattabile alle esigenze future. L'ottica rivolta al futuro è testimoniata anche dalla precisazione della possibilità per le persone di scegliere qualsiasi strumento comunicativo; non vengono formulati elenchi tassativi, ma si lascia spazio alle possibili evoluzioni tecnologiche. Vengono individuati tre nuclei fondamentali del diritto alla libera espressione, che restano immutabili indipendentemente dal mezzo di comunicazione prescelto: la libertà di condividere le proprie idee, di ricercare informazioni e di riceverle.

Il diritto alla condivisione viene confermato dal successivo art.27, secondo il quale ogni persona deve avere la possibilità di partecipare attivamente alla vita sociale, culturale e politica della propria comunità, di godere delle manifestazioni artistiche e dei benefici connessi al progresso scientifico. In altre parole, viene riconosciuto all'essere umano il diritto a godere dei risultati ottenuti attraverso la circolazione delle informazioni.

Come precedentemente accennato, l'affermazione dei diritti umani non è assoluta, ma circondata da alcuni limiti. L'art.29.2 della DUDU stabilisce che l'esercizio dei diritti stabiliti dalla Dichiarazione incontra i limiti previsti dalla legge per il riconoscimento e il rispetto delle libertà altrui, nonché per la salvaguardia di fattori determinanti come l'ordine e la sicurezza pubblica. Studiando la disposizione in esame, si nota che le limitazioni ammesse non sono tassative e predeterminate, ma sono modellabili a seconda

[286] P.E.ROZO SORDINI, *op.cit.,* pp.8.

delle esigenze della collettività a cui si riferiscono. Deve quindi procedersi a una valutazione del caso concreto; i confini della libertà di espressione non sono astrattamente individuabili e possono subire modifiche a seconda dei diversi contesti sociali, geografici e temporali in cui si colloca il suo esercizio.

Considerate le diverse opinioni in tema di diritti umani, si comprende il motivo per cui la DUDU non è uno strumento giuridicamente vincolante; è stata approvata infatti dall'Assemblea Generale delle Nazioni Unite attraverso una Risoluzione[287].

Nonostante la sua natura non obbligatoria, la Dichiarazione Universale dei Diritti dell'Uomo è diventata ben presto un elemento fondamentale del diritto internazionale, influenzando in maniera determinante le successive carte costituzionali e creando attorno ad essa un formidabile consenso, come si evince dalla prassi degli Stati e dalle pronunce di molte corti internazionali.

L'azione delle Nazioni Unite per la tutela dei diritti umani non si è fermata alla promulgazione della DUDU, come testimoniato dalla creazione della Commissione dei Diritti Umani (oggi rinominata Consiglio per i Diritti Umani).

2.1.1. Il lavoro del Consiglio per i Diritti Umani e dello Special Rapporteur sulla libertà di espressione

L'allora Commissione dei Diritti Umani è stata creata nel 1946 sulla base di quanto previsto dall'art.68 della Carta delle Nazioni Unite. Il suo scopo era quello di promuovere una visione basata sul rispetto e la salvaguardia dei diritti fondamentali; il primo passo per raggiungere questo ambizioso scopo fu proprio la redazione della DUDU.

Nel 1993 questo organo decise di creare la figura del Relatore Speciale (*Special Rapporteur*) sulla libertà di espressione e di opinione, al fine di indagare sull'effettivo rispetto di tale principio tra i Paesi membri delle Nazioni Unite.

Ai fini della presente trattazione, è utile soffermarci sul rapporto del 1998 avente ad oggetto la relazione tra tecnologie digitali e comunicazione[288]. La rete Internet venne

[287] Risoluzione 217 A (III) adottata il 10 dicembre 1948.
[288] Report of the Special Rapporteur, Mr. Abid Hussain, submitted pursuant to Commission on Human Rights resolution 1997/26 (Doc. E/CN.4/1998/40 del 28 gennaio 1998), https://digitallibrary.un.org/record/1494435 (consultato il 17 settembre 2019).

definita come intrinsecamente democratica, poiché offre ad un vasto pubblico nuove fonti di informazione e permette ai propri utenti di prendere parte ad un meccanismo di comunicazione con diffusione globale. Considerato ciò, gli Stati che impongono misure restrittive alla navigazione sul *web* vengono accusati di tenere un atteggiamento paternalistico, specialmente per la giustificazione addotta di voler così proteggere l'integrità morale della propria popolazione.

Queste limitazioni, nell'opinione dello *Special Rapporteur*, non riconoscono la possibilità per i cittadini di autodeterminare il proprio sviluppo civico e sociale, rappresentando un'intollerabile ingerenza nella loro sfera privata che è incompatibile con i principi di dignità e libertà della persona umana. La convinzione è che lo sviluppo del *public discourse* non richieda alcun intervento statale e che possa formarsi quindi in autonomia, secondo le libere determinazioni dei cittadini stessi.

L'attenzione delle Nazioni Unite al complesso rapporto tra nuove tecnologie e libertà di espressione ha portato al report del 2011 dello *Special Rapporteur* Frank LaRue[289]. Il rapporto ha rappresentato un vero e proprio punto di svolta nell'azione a difesa di uno spazio cibernetico aperto e fruibile per ogni utente, andando a influenzarne gli sviluppi internazionali successivi[290]. Partendo dall'analisi del ruolo avuto dalle reti digitali e dai *social media* nelle rivolte della cd. Primavera Araba[291], LaRue ha concluso che Internet è uno strumento fondamentale per la realizzazione di una vasta gamma di diritti fondamentali. Lo *Special Rapporteur* ha poi aggiunto che è ormai imprescindibile un'azione unitaria a livello globale volta ad assicurare a ogni essere umano la possibilità di accedere allo spazio cibernetico.

[289] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (Doc A/HRC/17/27 del 16 maggio 2011), https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (consultato il 17 settembre 2019).

[290] P.DE HERT, D.KLOZA, *Internet (access) as a new fundamental right. Inflating the current rights framework?*, in *European Journal of Law and Technology*, vol.3, n.3., 2012, pp.1-32

[291] Primavera Araba è l'espressione con cui solitamente si fa riferimento alle rivolte che hanno caratterizzato i Paesi arabi nel 2011, http://www.treccani.it/enciclopedia/primavera-araba/ (consultato il 17 settembre 2019).

2.2.Il riconoscimento nel Patto Internazionale sui Diritti Civili e Politici della libertà di espressione indipendentemente dal mezzo di comunicazione utilizzato

"*I membri della Commissione devono tenere in considerazione che il loro lavoro è rivolto verso il futuro e non verso il passato. Nessuno può prevedere come si evolveranno i mezzi di comunicazione nei secoli a venire."*[292] Il delegato francese si espresse con queste parole durante la stesura del Patto Internazionale sui Diritti Civili e Politici[293] (d'ora in poi anche il Patto o ICCPR); l'intento era quindi di formulare previsioni in tema di diritti fondamentali che non risentissero dello scorrere del tempo, ma che mantenessero intatta la propria validità ed efficacia nel corso degli anni.

L'art.19 del Patto è stato chiaramente influenzato da quanto stabilito dal medesimo articolo della DUDU, poiché afferma la valenza globale del diritto alla libera espressione. La scelta delle parole utilizzate nella formulazione di detto articolo non è certamente causale, e rispecchia quanto auspicato dal delegato francese. Si parla infatti di un diritto a ricercare, ricevere e importare (*seek, receive* e *import* nella stesura originale del testo in lingua inglese) informazioni di ogni tipo, indipendentemente da frontiere o barriere di qualsiasi specie.

I termini utilizzati rendono l'articolo 19 del Patto ancora attuale, anche nel contesto cibernetico; descrivono in maniera efficace il comportamento di un utente cibernetico che ricerca informazioni nel *web*, che le condivide e/o le scarica sul proprio dispositivo elettronico. La rilevanza attuale della disposizione in questione risulta ancora più evidente se si osserva la specificazione secondo la quale tali diritti sono valevoli in maniera indipendente dal mezzo di comunicazione scelto. All'epoca della stesura dell'ICCPR si è quindi deciso di non proporre un elenco tassativo di strumenti utilizzabili per comunicare, ma si è consapevolmente scelto di lasciare libero spazio alle possibili evoluzioni tecnologiche.

Analogamente a quanto stabilito dalla DUDU, il Patto elenca una serie di possibili limitazioni al diritto alla libera espressione, ponendo però dei requisiti alquanto stringenti.

---

[292]Consiglio per i Diritti Umani delle Nazioni Unite, sesta sessione, 165esimo meeting, 2 maggio 1950, http://hr-travaux.law.virginia.edu/document/iccpr/ecn4sr165/nid-1732 (consultato il 17 settembre 2019).

[293] Il Patto Internazionale sui Diritti Civili e Politici è un trattato multilaterale adottato dall'Assemblea Generale delle Nazioni Unite con la Risoluzione 2200A (XXI) il 16 dicembre 1966. Il testo del trattato è disponibile al seguente link https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf (consultato il 17 settembre 2019).

L'art.19 sez.III afferma infatti che tali restrizioni devono essere formulate in maniera chiara e non arbitraria. Devono essere inoltre "*espressamente stabilite dalla legge e risultare indispensabili per a) assicurare il rispetto dei diritti o della reputazione altrui; b) la protezione della sicurezza nazionale, l'ordine pubblico, la salute o la morale pubbliche"*. A propositi dei criteri appena citati, occorre menzionare che spetta allo Stato dimostrare la necessarietà delle misure eventualmente approntate a limitazione della libera espressione dei propri cittadini.

Proseguendo nell'analisi delle disposizioni del Patto in merito alla libertà di parola, giova citare l'articolo 17 che, riprendendo quanto riconosciuto anche dalla precedente DUDU, afferma che "*nessuno può essere oggetto di (...) attacchi al proprio onore e reputazione*" e che "*ogni persona ha diritto ad essere protetto dalla legge contro tali ingerenze e attacchi*". L'art.20 proclama il divieto di discriminazione, asserendo che "*ogni forma d'incitamento all'odio basato sull'appartenenza a uno Stato, a una razza o religione sarà proibito dalla legge*". Questa disposizione ha una particolare valenza per quanto riguarda il contesto cibernetico, visto che si oppone all'odioso fenomeno del cd.*hate speech*, o propaganda d'odio, di cui si dirà diffusamente più avanti.

Per quanto riguarda l'effettiva applicazione di quanto previsto dal Patto, il Comitato dei Diritti Umani avrebbe dovuto giudicare sui ricorsi presentati da uno Stato membro nei confronti di un'altra parte contraente; questo particolare meccanismo giurisdizionale non è poi entrato in funzione a causa del disaccordo tra i Paesi coinvolti. Il Protocollo Alternativo[294] del 1976 ha permesso a soggetti privati di presentare ricorsi contro Stati membri accusati di aver violato disposizioni dell'ICCPR; una volta esauriti i ricorsi interni, il privato può infatti far valere le proprie posizioni davanti al Comitato. Questo organo ha il compito di interessare lo Stato coinvolto, dandogli 6 mesi di tempo per rispondere alle questioni sollevate. Successivamente lo stesso Comitato esprime il proprio parere (non vincolante) sulla controversia; lo Stato ha comunque l'obbligo di comunicare le soluzioni intraprese.

L'importanza della condivisione delle informazioni nelle materie scientifiche e culturali è ben presente anche nella formulazione dell'art.19 del Patto Internazionale sui Diritti economici, sociali e culturali (anche ICESCR)[295]. La disposizione in questione

[294] Protocollo Alternativo al Patto Internazionale sui Diritti Civili e Politici, https://www.ohchr.org/EN/ProfessionalInterest/Pages/OPCCPR1.aspx (consultato il 17 settembre 2019).
[295] Patto Internazionale sui Diritti economici, sociali e culturali, adottato dall'Assemblea Generale delle Nazioni Unite con la Risoluzione 2200A(XXI) il 16 dicembre del 1966, https://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx (consultato il 18 settembre 2019).

impegna gli Stati membri del trattato a diffondere la scienza e la cultura, rispettando la libertà di ricerca scientifica e ogni altra attività creativa. Per raggiungere questi ambiziosi risultati occorre che il diritto alla libera espressione sia effettivamente salvaguardato e tutelato.

2.3. La tutela del diritto alla libera espressione negli accordi regionali

La libertà di pensiero e di parola, come si accennava poc'anzi, è ormai parte integrante del diritto internazionale. Questa realtà è confermata dal fatto che numerosi accordi interstatali a livello regionale riconoscono il diritto alla libera espressione come un principio imprescindibile per l'essere umano. Diversi trattati in Europa, America e Africa si sono pronunciati in tal senso, garantendo inoltre la riservatezza delle comunicazioni tra le persone.

Risulta particolarmente significativa la mancanza di un accordo regionale con simili contenuti per il continente asiatico: questa è un'ulteriore testimonianza di come la libertà di espressione non può essere (ancora) definita in maniera uniforme a livello globale, dati i diversi contesti sociali e culturali.

I trattati regionali di cui si darà brevemente conto si contraddistinguono per una caratteristica comune, ossia la possibilità di ottenere un controllo giurisdizionale su tutte quelle azioni che limitano la libertà di espressione.

2.3.1. Il diritto alla libera espressione nell'azione del Consiglio di Europa e il suo riconoscimento nel diritto europeo primario

Il primo accordo regionale a cui si vuole far riferimento è la Convenzione europea per la protezione dei diritti umani e le libertà fondamentali (anche CEDU)[296], adottata nel 1950 in seno al Consiglio di Europa.

L'articolo 10 di questo trattato riconosce a ogni essere umano il diritto alla libera espressione, aggiungendo che tale diritto si concretizza anche nella possibilità di ricevere e condividere informazioni (*receive* e *impart* nel testo originale in lingua inglese) senza dover tenere conto di confini o barriere. Il secondo paragrafo del medesimo articolo

[296] Il testo della Convenzione europea per la protezione dei diritti umani e le libertà fondamentali è disponibile al seguente link https://www.echr.coe.int/Documents/Convention_ITA.pdf (consultato il 18 settembre 2019).

afferma il carattere non assoluto di questo diritto, aggiungendo che può essere sottoposto a limitazioni e restrizioni in virtù di norme previste dalla legge e necessarie in una società democratica per il perseguimento di interessi quali, ad esempio, la sicurezza nazionale, l'integrità territoriale, il mantenimento dell'ordine pubblico e la tutela della pubblica morale.

Ad una prima lettura dell'articolo in esame risulta evidente che la CEDU vuole tutelare anche le comunicazioni internazionali: la condivisione delle informazioni attraverso lo spazio cibernetico rientra sicuramente in tale ambito. Queste restrizioni devono però rispettare criteri stringenti: lo stesso articolo afferma infatti che devono essere considerate necessarie per il mantenimento di una società democratica e devono essere altresì previste da apposite norme di legge. Si vuole perciò limitare possibili comportamenti abusivi da parte dello Stato e dei pubblici poteri. L'applicazione delle eccezioni appena menzionate deve essere valutata sulla base del caso concreto e la loro legittimità non può quindi essere decisa in maniera astratta e aprioristica.

L'articolo 10 deve essere letto e applicato in combinato disposto con il successivo articolo 17, il quale prevede che nessun diritto riconosciuto dalla CEDU permette di compiere azioni che vanno contro lo spirito della Convenzione stessa, violando altri diritti sanciti da questa. Si applica perciò un sistema di *checks and balances*, ossia di pesi e contrappesi, che vuole mantenere un equilibrio nell'esercizio dei diritti e nel rispetto delle libertà di ogni individuo appartenente alla collettività sociale.

Molti Paesi che hanno preso parte alla CEDU hanno recepito le sue disposizioni all'interno del proprio ordinamento nazionale, permettendo che le disposizioni della Convenzione siano invocate di fronte ai giudici statali.

Per quanto riguarda il controllo giurisdizionale sul rispetto effettivo delle norme CEDU, si deve far riferimento all'operato della Corte europea dei diritti dell'uomo. La possibilità di far ricorso contro eventuali violazioni della Convenzione è garantita anche ai singoli individui, a patto che abbiano preventivamente esaurito ogni forma di ricorso interno e abbiano presentato in via preliminare istanza di fronte alla Commissione europea dei diritti umani. Questo apposito organo è infatti preposto a decidere sull'ammissibilità dei ricorsi, prima che questi vengano effettivamente presentati ai giudici. Le sentenze della Corte hanno carattere vincolante, sebbene non siano in grado di annullare/revocare eventuali decisioni di autorità nazionali. Vengono comunemente irrogate sanzioni pecuniarie nei confronti degli Stati ritenuti colpevoli di aver violato delle norme CEDU.

Il diritto alla libera espressione ha poi ricevuto riconoscimento di rango primario all'interno dell'ordinamento dell'UE. L'art.11 della Carta dei diritti fondamentali dell'Unione europea[297] (anche carta di Nizza) assicura a ogni cittadino il diritto di esprimersi liberamente e di condividere informazioni, senza alcuna restrizione basata sulle frontiere e senza ingerenze da parte dei pubblici poteri. Si garantisce inoltre il rispetto dell'indipendenza e del pluralismo dei mezzi di comunicazione. L'articolo 6 del Trattato sull'Unione europea[298], così come modificato dagli accordi di Lisbona del 2009, afferma che la UE riconosce i diritti, le libertà e i principi della Carta di Nizza garantendo a questi il medesimo valore giuridico dei Trattati istitutivi. In altre parole, hanno valore primario e vincolano l'azione dell'Unione europea per quanto riguarda l'emanazione e l'attuazione del diritto secondario o derivato.

La Corte di giustizia dell'Unione europea può quindi essere chiamata a giudicare su eventuali violazioni di quanto previsto dalla Carta di Nizza nei limiti stabiliti dalla Carta stessa.

2.3.2. La Carta di Parigi a tutela della libertà di espressione

L'incontro dei Capi di Stato e di governo tenutosi a Parigi nel novembre 1990 nell'ambito della Conferenza sulla Sicurezza e la Cooperazione in Europa ha prodotto la cd. Carta di Parigi per una nuova Europa (anche Carta di Parigi)[299]. Si tratta di una dichiarazione di intenti secondo la quale ogni individuo "*ha diritto alla libertà di pensiero, coscienza, religione o credo e alla libertà di espressione*". Si riconosce l'importanza del pluralismo dei mezzi di informazione per garantire la formazione di una coscienza pubblica in maniera autonoma e indipendente. Le tecnologie digitali, e in particolar modo Internet, vengono definite come gli strumenti maggiormente in grado di salvaguardare detto pluralismo, proprio per le loro caratteristiche ontologiche; si pensi alla diffusione globale della rete e alla relativa disponibilità a prezzo economico di *device* per la connessione. Considerato ciò, gli Stati devo impegnarsi a garantire ai propri cittadini la possibilità di scegliere tra diverse fonti di informazione indipendenti e

[297] Il testo della Carta dei diritti fondamentali dell'Unione europea, nella traduzione ufficiale italiana, è disponibile al seguente link https://www.europarl.europa.eu/charter/pdf/text_it.pdf (consultato il 20 settembre 2019).
[298] Trattato sull'Unione europea, in GUUE C 326/13 del 26 ottobre 2012, pp.1-34.
[299] La versione italiana del testo della Carta di Parigi per una nuova Europa è disponibile al seguente link https://www.osce.org/it/mc/39519?download=true (consultato il 18 settembre 2019).

imparziali. Sono comunque mantenute le consuete restrizioni per il diritto alla libera espressione, che può essere limitato da norme previste dalla legge o per il rispetto delle disposizioni di accordi internazionali.

2.3.3. La difesa della libertà di espressione nel continente africano: la Carta africana dei diritti dell'uomo e dei popoli

La necessità di arrivare a una Convenzione africana in materia di diritti umani emerge chiaramente dalle risultanze del congresso dei Giuristi africani del 1961, ma viene recepita solamente nel 1979 dall'Assemblea dei Capi di Stato e di governo dell'Organizzazione dell'Unità Africana (OUA). Il risultato di questa presa di posizione è la Carta africana dei diritti dell'uomo e dei popoli, nota anche come Carta di Banjul dal nome della città del Gambia dove venne redatta nel 1981 la sua versione finale[300]. La quasi totalità degli Stati appartenenti all'OUA ha ratificato la Carta: allo stato attuale manca solamente la firma della neonata Repubblica del Sud Sudan, diventata membro dell'Organizzazione dell'Unità Africana nel 2011.

Il termine utilizzato per descrivere il documento in questione, "Carta", può risultare fuorviante; si dovrebbe più propriamente parlare di Convenzione, dato il carattere vincolante che questo ha per i membri firmatari. Si tratta di un elenco di diritti civili, politici, economici e culturali che si presentano come indissolubilmente legati e imprescindibili per il corretto sviluppo della popolazione africana.

Un elemento di novità apportato dalla Carta di Banjul rispetto ai precedenti atti internazionali in tema di diritti umani è la previsione di diritti collettivi o diritti dei popoli; con questi termini si vuole intendere sia il diritto all'autodeterminazione politica ed economica che il diritto allo sviluppo e alla pace. Un altro profilo innovativo è dato dalla presenza di ben 3 articoli (27-29) che enucleano una serie di doveri per l'individuo, diretti verso 5 collettività distinte: a) famiglia b) società c) Stato d) altri gruppi sociali riconosciuti e) comunità internazionale. Questi doveri si concretizzano nel mantenere la pace e l'armonia tra i membri dei vari gruppi, contribuendo con la propria attività allo sviluppo dell'intera collettività.

Tornando al tema della presente trattazione, l'art.9 della Carta di Banjul attribuisce a ogni persona il diritto all'informazione e ad esprimere la propria opinione

[300] Una traduzione italiana del testo della Carta africana dei diritti dell'uomo e dei popoli è disponibile al seguente link http://ospiti.peacelink.it/cd/docs/1141.pdf (consultato il 18 settembre 2019).

nel rispetto della legge e dei regolamenti vigenti. I Paesi firmatari hanno inoltre il dovere di promuovere e far rispettare i diritti sanciti dalla Carta. Per quanto riguarda eventuali limitazioni all'esercizio di tali diritti, queste vengono trovate nel rispetto delle libertà altrui e nel mantenimento della salute e della sicurezza pubblica, come sancito dall'art.27.

2.3.4. Gli accordi regionali nel continente americano a difesa della libertà di espressione

Il dibattito intorno alla tutela dei diritti fondamentali è sempre stato al centro dell'attenzione politica e giuridica del continente americano, come testimoniato dalla Dichiarazione americana dei diritti e doveri dell'uomo[301] (anche Dichiarazione americana), che è stato il primo documento internazionale a difesa dei diritti umani, anteriore di alcuni mesi alla Dichiarazione universale.

Il testo in esame è stato adottato come strumento di *soft law*, dotato quindi di valore dichiarativo e non vincolante; lo scopo originario era quello di fornire le linee guida per l'azione della neonata Organizzazione degli Stati americani (OSA). Può essere interessante notare il particolare accorgimento adottato per far sì che la Dichiarazione americana potesse risultare funzionale anche in un'ottica futura: il considerando IV definisce il documento in questione come una forma iniziale di protezione dei diritti fondamentali strettamente legata alle concezioni e alle esigenze sociali dell'epoca, non escludendo però che tale sistema di tutela si sarebbe potuto rafforzare in presenza di condizioni più favorevoli in futuro.

Tali circostanze si sono poi effettivamente presentate: l'Assemblea Generale dell'OSA ha più volte sottolineato[302] nel corso degli anni che gli Stati membri hanno degli obblighi precisi nel rispetto di quanto stabilito dalla Dichiarazione Americana.

Tornando al tema principale della nostra analisi, si vuole concentrare l'attenzione sull'articolo IV del testo in questione, il quale afferma che ogni persona ha diritto alla

[301] Il testo della Dichiarazione americana dei diritti e doveri dell'uomo, approvato durante la nona Conferenza Internazionale degli Stati americani, tenutasi a Bogotà nel 1948, è disponibile al seguente link https://www.oas.org/dil/access_to_information_human_right_American_Declaration_of_the_Rights_and_Duties_of_Man.pdf (consultato il 19 settembre 2019).

[302] Si fa qui riferimento a tre diverse Risoluzioni: a) la Risoluzione 314 (VII-O/77) del 22 giugno 1977 con ela quale gli Stati incaricavano la Commissione interamericana di approntare un'indagine conoscitiva in merito agli effettivi obblighi per i Paesi membri scaturenti dal rispetto della Dichiarazione americana; b) la Risoluzione 371 (VIII-O/78) del 1 luglio 1978 in cui l'Assemblea generale afferma nuovamente l'impegno nel tutelare i diritti sanciti dalla Dichiarazione americana; c) la Risoluzione 370 (VIII-O/78) del 1 luglio 1978 in cui viene annoverato tra gli obblighi internazionali di uno Stato membro dell'OSA il rispetto di quanto proclamato dalla Dichiarazione americana.

libertà di espressione attraverso qualsiasi mezzo. La decisione di non limitare tale libertà all'utilizzo di specifici strumenti rende questa disposizione attuabile anche nel contesto cibernetico.

Continuando lo studio dei documenti regionali in tema di tutela dei diritti fondamentali, occorre ricordare la Convenzione americana sui diritti umani[303], nota anche come Patto di San Josè dal nome della città in cui è stata redatta nel 1969. Secondo quanto previsto dal testo in esame, gli Stati firmatari si impegnano a rispettare e garantire i diritti che sono sanciti dalla Convenzione stessa. L'articolo 2 prevede infatti che i Paesi parte del trattato debbano conformare il proprio ordinamento interno alle disposizioni del Patto. Per assicurare l'effettiva tutela dei diritti sanciti dalla Convenzione, è stata istituita la Corte interamericana dei diritti come organo giudiziario indipendente; 24 degli Stati firmatari del trattato hanno riconosciuto la giurisdizione della Corte come vincolante.

Per quanto riguarda la salvaguardia della libera espressione, si deve tenere conto di quanto disposto dall'art.13. L'articolo in questione, oltre a sancire il diritto alla libertà di informazione e di parola per ogni persona, si distingue dai documenti precedentemente esaminati per diversi aspetti innovativi. Si statuisce che la libertà di espressione non può essere sottoposta a censura preventiva, garantendo inoltre il diritto di replica a qualsiasi persona si senta in qualche modo oltraggiata dalla condivisione e diffusione di una specifica informazione. Vengono poi vietate le limitazioni indirette, come controlli abusivi sulla stampa o sulle frequenze radiotelevisive.

3. La responsabilità degli Internet Service Provider nella tutela del diritto alla libera espressione nella giurisprudenza della Corte di giustizia dell'Unione europea.

Si è vista l'attenzione europea riservata al delicato tema della tutela dei diritti fondamentali; si tratta però di un atteggiamento relativamente recente. A tal proposito, bisogna considerare che la nascita dell'Unione europea trova le sue originarie motivazioni in ragioni strettamente economiche, più che nella salvaguardia dei diritti umani.

Una diretta conseguenza di questa realtà è data dal fatto che la Corte di giustizia dell'Unione europea si è trovata raramente a doversi pronunciare direttamente in merito

[303] Il testo ufficiale della Convenzione americana sui diritti umani è disponibile al seguente link https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm (consultato il 20 settembre 2019).

alla salvaguardia della libera espressione o di altri principi fondamentali. I giudici erano invece sovente chiamati a giudicare se le limitazioni poste a determinate libertà economiche per la tutela di specifici diritti umani fossero o meno giustificate[304].

La pronuncia *Zenatti*[305] è un chiaro esempio di questa situazione, dove la Corte è stata chiamata a valutare le conseguenze della navigazione cibernetica sull'effettivo rispetto delle prerogative di natura economica riconosciute dai Trattati istitutivi dell'Unione europea. L'elemento di controversia nel caso in questione era dato dall'eventuale contrasto tra la normativa italiana, che riservava la possibilità di organizzare scommesse e giochi di azzardo ad alcuni enti riconosciuti dallo Stato, e il diritto alla libera prestazione di servizi affermato dalla normativa primaria europea. Il signor Zenatti operava come intermediatore per un *bookmaker* britannico non abilitato ad esercitare la sua professione sul suolo italiano.

Un'ulteriore occasione di bilanciamento tra libertà economiche e valori fondamentali si è avuto con la sentenza *Omega*[306] : nel caso in questione i giudici erano chiamati a pronunciarsi sulla compatibilità con il diritto dell'Unione europea di un provvedimento tedesco con cui si vietava la vendita di un videogioco dai contenuti particolarmente violenti, al fine di preservare la morale pubblica. La Corte di giustizia ha riconosciuto che la libertà di iniziativa economica deve comunque coesistere con la salvaguardia e il mantenimento dell'ordine pubblico. La tutela della dignità umana, cui anche l'ordinamento UE è preordinato, non può essere messa in ombra da motivazioni di mero carattere economico.

Proseguendo nell'analisi della giurisprudenza della Corte in merito alla ricerca di un punto di equilibrio tra diversi diritti parimenti meritevoli di tutela, occorre discutere brevemente della sentenza *Google*[307]. In tale occasione, i giudici hanno avuto modo di riflettere sul ruolo dei cd. *Internet Service Provider* (ISP) nell'architettura dello spazio cibernetico e su come questo si sia costantemente evoluto al ritmo del continuo progresso tecnologico. La direttiva 2000/31/CE sul commercio elettronico[308] esclude, al ricorrere di

---

[304] O.POLLICINO, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in (a cura di) V.BARSOTTI, *Libertà di informazione, nuovi mezzi di comunicazione e tutela dei diritti,* Firenze, 2014, pp.101-128.

[305] Corte di giustizia dell'Unione europea, sentenza del 21 ottobre 1999, *Zenatti*, causa C-67/98.

[306] Corte di giustizia dell'Unione europea, sentenza del 14 ottobre 2004, *Omega*, causa C-36/02, ECLI:EU:C:2004:614

[307] Corte di giustizia dell'Unione europea, sentenza del 23 marzo 2010, *Google*, cause riunite da C-236/08 a C-238/08, ECLI:EU:C:2010:159.

[308] 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 («Direttiva sul commercio elettronico»).

determinate condizioni, la responsabilità degli ISP per le condotte illecite poste in essere dagli utenti qualificando gli intermediari informatici come semplici prestatori di servizi. Solamente nel caso in cui la loro opera non rientri esclusivamente nell'ambito dell'intermediazione, scatta una responsabilità simile a quella editoriale. La direttiva appena presa in considerazione fa però riferimento a un'epoca in cui la circolazione delle informazioni attraverso il *cyberspace* seguiva altre modalità e differenti velocità rispetto a quelle odierne. Le grandi piattaforme informatiche di condivisione dei contenuti non avevano ancora raggiunto il loro pieno potenziale. La Corte di giustizia ha quindi cercato di tenere il passo dell'avanzamento delle nuove tecnologie delineando i limiti delle responsabilità degli ISP. I fatti di causa avevano ad oggetto un servizio pubblicitario a pagamento attraverso la selezione di determinate parole chiave, chiamato anche *keyword advertising*. La controversia era sull'effettiva responsabilità in capo al prestatore di servizi della visualizzazione, ottenuta grazie all'inserimento di dette parole specifiche facenti riferimento al marchio che si voleva pubblicizzare, di prodotti non contenenti tale segno distintivo, in quanto imitazioni. Le alternative di fronte alla Corte erano sostanzialmente due: ritenere responsabile l'ISP dell'operato di tale servizio di *keyword advertising* o esonerarlo invece da qualsiasi responsabilità in quanto questo procedimento informatico era totalmente automatico e non abbisognava di alcun intervento esterno.

I giudici hanno risolto la controversia applicando il parametro enunciato dall'art.14 della direttiva sul commercio elettronico in merito alle possibili esenzioni di responsabilità per i *provider*. Qualora l'ISP si limiti a un supporto tecnico, passivo e automatico, non dovrà essere chiamato a rispondere delle sue azioni. Diverso è il caso in cui tale soggetto intervenga attivamente nella selezione dei contenuti da immettere nello spazio cibernetico e nella scelta delle modalità di condivisione.

Pur non concernendo direttamente la tematica del diritto alla libera espressione, la sentenza *Google* è interessante ai fini della presente trattazione per lo sforzo della Corte di offrire un'interpretazione della normativa vigente coerente con il progresso delle nuove tecnologie[309].

Questo atteggiamento si riscontra anche nella sentenza *l'Oréal*[310] dove i giudici del Lussemburgo sono stati chiamati a giudicare l'effettiva responsabilità di un noto sito di *e-commerce* per quanto riguarda gli annunci di vendita di prodotti contraffatti postati

[309] O.POLLICINO, *op.cit.*
[310] Corte di giustizia dell'Unione europea, sentenza del 12 luglio 2011, *l'Oréal,* causa C-324/09, ECLI:EU:C:2011:474.

da utenti cibernetici su detta piattaforma informatica. Nel caso in questione, la Corte di giustizia ha qualificato l'operato del portale digitale come mero *hosting*, qualificandolo quindi come intermediario e inserendolo nelle categorie di esenzioni di cui alla direttiva 2000/31/CE sul commercio elettronico. L'attenzione dei giudici della Corte, come nel caso precedentemente esaminato, è rivolta alla tutela dell'iniziativa economica senza approfondire le possibili tematiche in merito agli altri valori fondamentali che potrebbero venire in considerazione.

La prospettiva prevalentemente economica-industriale nel ragionamento della Corte caratterizza anche la sentenza *Promusicae*[311]: in questa occasione la controversia verteva sull'effettiva legittimità della raccolta dei dati personali degli utenti da parte di ISP per la finalità di combattere la "pirateria" musicale e le sistematiche violazioni del diritto di autore compiute attraverso portali di *peer-to-peer*. I giudici hano preso in considerazione non tanto la possibile violazione della privacy degli utenti in quanto tale, ma l'auspicato bilanciamento tra la possibile lesione della loro autonomia informativa con gli interessi economici dei detentori del diritto alla proprietà intellettuale sulle canzoni trasmesse via *web.*

La tutela dei diritti fondamentali, e in particolar modo della libera espressione, assume autonoma rilevanza nelle sentenze *Sabam*[312]. Oggetto di controversia era la possibilità di obbligare gli *ISP* (nel procedimento *Scarlet*) e i gestori delle piattaforme di *social media* (nel caso *Netlog*) ad adottare particolari sistemi di filtraggio dati volti a impedire atti di violazione del diritto di autore attraverso Internet. L'imposizione di tali obblighi avrebbe potuto comportare importanti conseguenze sulla libertà di espressione dei singoli utenti cibernetici.

La Corte, nelle sentenze in esame, ha riconosciuto che la finalità ultima di garantire il rispetto delle norme del diritto di autore non può portare a trasformare l'effettivo ruolo degli ISP. Seguendo questo ragionamento, si conclude che gli intermediari non possono essere gravati di un obbligo di adottare dei sistemi di filtraggio delle informazioni che comporterebbero la sorveglianza dell'attività degli utenti informatici e vanificherebbero di conseguenza il loro diritto alla libera espressione.

[311] Corte di giustizia dell'Unione europea, sentenza del 29 gennaio 2008, *Promusicae*, causa C-275/06, ECLI:EU:C:2008:54.
[312] Corte di giustizia dell'Unione europea, sentenza del 24 novembre 2011, *Scarlet Extended SA c. SABAM*, causa C-70/10; sentenza del 16 febbraio 2012, *SABAM c. Netlog NV*, causa C-360/10, ECLI:EU:C:2012:85.

Come anticipato poc'anzi, i giudici della Corte operano una sorta di bilanciamento tra i diversi interessi in gioco; le modalità scelte per raggiungere questo punto di equilibrio meritano una particolare attenzione. Nella sentenza *Scarlet*, la Corte sottolinea l'importanza del diritto alla proprietà intellettuale, tutelato dall'articolo 17 della Carta dei diritti fondamentali dell'Unione europea e del suo bilanciamento con gli altri interessi parimenti meritevoli di salvaguardia. La libertà di iniziativa economica dei *provider*, protetta dall'articolo 16 della Carta di Nizza, risulterebbe lesa dall'eventuale obbligo loro imposto di adottare un sistema permanente di filtraggio, che sarebbe eccessivamente costoso per le finalità perseguite. Solamente in seconda battuta i giudici valutavano l'impatto che tale sistema avrebbe per il diritto degli utenti cibernetici all'autonomia informativa (art.8 della Carta) e a condividere informazioni (art.11 della Carta).

Bisogna però notare come, nonostante importanti valori quali il diritto alla privacy e all'informazione siano stati effettivamente presi in considerazione dal *reasoning* della Corte, il primo pensiero dei giudici sia stato rivolto, in entrambe le sentenze *Sabam*, alla tutela della libera iniziativa imprenditoriale dei *provider*; il che evidenzia che il punto di vista economico rimane prevalente. Nelle pronunce in esame, non si è avuta inoltre una chiara presa di posizione in merito ai possibili rischi informatici per il diritto alla libera espressione e sul rapporto di tale principio con il diritto di autore[313].

La Corte si limita a precisare che le possibili misure adottate dall'ISP per far cessare eventuali violazioni di *copyright* devono essere mirate e proporzionate allo scopo, senza però specificare effettivamente quali caratteristiche devono essere rispettate.

La breve analisi qui riportata della giurisprudenza della Corte di giustizia più rilevante in materia di tutela del diritto alla libera espressione ci permette di proporre alcune riflessioni conclusive.

In materia di salvaguardia dei diritti fondamentali, l'Unione europea ha iniziato la propria azione solamente in un'epoca relativamente recente, scontando un congenito ritardo dovuto alla sua nascita per esclusive finalità economiche (si pensi a tal proposito alla CECA prima e alla CEE poi). Questa realtà dei fatti è comprovata anche dall'azione dei giudici della Corte UE, la cui giurisprudenza sopra esaminata evidenzia come la loro

[313] A.SPAGNOLO, *Bilanciamento tra libertà d'espressione su Internet e tutela del diritto d'autore nella giurisprudenza recente della Corte europea dei diritti umani*, in www.federalismi.it, 17 maggio 2013, p. 9, https://federalismi.it/nv14/articolodocumento.cfm?Artid=22426&content=Bilanciamento+tra+libert%25C3%25A0+d%25E2%2580%2599espressione+su+internet+e+tutela+del+diritto+d%25E2%2580%2599autore+nella+giurisprudenza+recente+della+Corte+europea+dei+diritti+umani&content_author=Andrea+Spagnolo (consultato il 23 settembre 2019).

attenzione ai diritti fondamentali sia solitamente volta a un bilanciamento di questi ultimi con diritti e libertà economiche.

4. I limiti della libera espressione nel contesto cibernetico secondo la giurisprudenza della Corte europea dei diritti umani e della Corte di giustizia dell'Unione europea

La giurisprudenza della Corte EDU in materia di tutela della libera espressione presenta caratteristiche ben distinte da quella della Corte di giustizia. I giudici di Strasburgo, piuttosto che concentrarsi sull'equilibrio tra libertà economiche e diritti fondamentali, hanno concentrato la loro attenzione sull'analisi degli effettivi limiti alla libera espressione nel contesto cibernetico, cercando di comprendere quanto le tradizionali categorie giuridiche potessero rivelarsi adatte anche al mondo *on-line*.

Nel caso *Handyside c. Regno Unito*[314] la Corte EDU ha avuto modo di dichiarare che la libertà di espressione è uno dei capisaldi della società democratica e un elemento imprescindibile per il suo concreto sviluppo. L'art.10 della CEDU è necessario per tutelare non tanto le opinioni maggioritarie, ma soprattutto i pensieri che si differenziano rispetto al sentimento dominante; i giudici confermano perciò la dimensione antagonista del diritto alla libertà di parola. Nella medesima pronuncia, i giudici elaborano una formula ancora utilizzata per valutare la legittimità delle limitazioni statali all'esercizio della libera espressione da parte dei singoli cittadini. Queste ingerenze devono essere 1) riconosciute dalla normativa vigente, 2) avere come finalità ultima un obbiettivo non contrario a quanto previsto dall'art.10 CEDU e 3) necessarie in una società democratica; non a caso si parla di *triple test clause*[315].

L'adozione di questa formula ha permesso di porre un freno alle possibili ingerenze dei pubblici poteri in merito alla libertà di comunicazione, incentivando così il pluralismo dei *media*, specialmente nei Paesi che hanno aderito al Consiglio di Europa in seguito alla caduta del muro di Berlino[316]. Chiamata a valutare casi riguardanti limitazioni

[314] Corte EDU, sent. 7 dicembre 1976, ricorso n. 5493/72, *Handyside c. Regno Unito.*
[315] S.GREER, *The exceptions to art.8 to 11 of the European Convention on Human Rights*, https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf (consultato il 23 settembre 2019).
[316] D.VOORHOOF, *Freedom of expression under the European Human Rights system*, in (a cura di) Y.HAECK, H.OLASOLO, J.VARVAELE, L.ZWAAK, *Inter-American and European Human Rights Journal*, 2009, pp.3-5.

al diritto alla libera espressione, la Corte EDU ha assunto un ruolo di supervisione in materia, così come effettivamente previsto dalla CEDU che aveva predisposto tale controllo giurisdizionale come ulteriore livello di salvaguardia per la tutela dei diritti umani in Europa[317].

I giudici di Strasburgo hanno comunque riconosciuto agli Stati un certo margine di apprezzamento nella valutazione dell'effettiva necessarietà di limitazioni e ingerenze rispetto alla condivisione delle informazioni da parte dei propri cittadini. Questo conferma il carattere relativo e non assoluto del diritto alla libera espressione, che trova il suo contraltare in principi quali la moralità e l'ordine pubblico. Alcune forme di espressione possono essere perciò limitate a seconda di determinate circostanze locali e, nel frattempo, comunemente accettate in altre evenienze temporali o geografiche. Considerato ciò, il requisito della necessarietà in una società democratica di cui si parlava poc'anzi in merito alla *triple test clause*, non diventa altro che un criterio di proporzionalità con cui valutare la restrizione alla libera espressione messa in atto rispetto alle finalità effettivamente perseguite. La Corte EDU, per valutare questo criterio, ha fatto riferimento a due aspetti specifici; la natura della limitazione apportata dallo Stato e la sua intensità.

Le eccezioni alla libera comunicazione devono essere però limitate e non andare contro lo spirito della Convenzione stessa e la sua propensione in favore al diritto alla libertà di espressione[318]; devono perciò rispettare quanto previsto dall'art.17 della CEDU. La norma in questione, a cui si era brevemente già accennato, stabilisce che non può essere permessa alcuna azione volta a impedire l'esercizio di diritti e libertà a terze parti, anche se tale azione è formalmente rispettosa di quanto statuito dalla CEDU[319].

La ragione di questa disposizione si trova nel periodo in cui è stata firmata la Convenzione, ossia nel secondo dopoguerra. L'intento alla base dell'articolo 17 è quello di prevenire la nascita di nuovi movimenti di odio e discriminazione come quelli che avevano portato allo scoppio del conflitto mondiale; partiti politici formalmente legittimi ed espressione quindi del diritto alla libera determinazione politica dell'essere umano, ma concretamente contrari a una società democratica basata sul rispetto dei diritti umani.

---

[317] O.POLLICINO, M.BASSINI, *Free speech, defamation and the limits to freedom of expression in the EU: a comparative analysis*, in (a cura di) A.SAVIN, J.TRZASKOWSKI, *Research Handbook on EU Internet Law*, 2014, Londra, pp.508-526.

[318] E.BARENDT, *Freedom of speech*, Oxford, 2007, pp.65.

[319] M.VILLINGER, *Article 17 ECHR and freedom of speech in Strasbourg practice*, in (a cura di) J.CASADEVALL, E.MVJER, M.O'BOYLE, A.AUSTIN, *Freedom of expression. Essays in honour of Nicolas Bratza*, Londra, 2012, pp. 321 ss.

La Corte EDU ha frequentemente utilizzato l'articolo 17 in combinato disposto con quanto previsto dall'art.10.2 allo scopo di determinare se una limitazione all'esercizio della libera espressione fosse effettivamente necessaria al mantenimento di un ordine democratico all'interno della collettività sociale[320]. Ha anche funzionato come elemento ulteriore nella ricerca di un punto di equilibrio tra il diritto alla libertà di parola e altri interessi parimenti meritevoli di tutela.

Non sono rari i riferimenti esclusivi all'articolo 17, specialmente nei casi in cui è stato negato che la comunicazione oggetto di controversia potesse essere tutelata da quanto previsto dalla CEDU. Si è parlato a tal proposito di "effetto ghigliottina", poiché l'informazione al centro della questione viene per l'appunto eliminata senza ulteriori discussioni[321]. Si può riscontrare tale effetto soprattutto nei giudizi in merito alla negazione dell'Olocausto; in tali occasioni la Corte ha solitamente seguito due strade, applicando direttamente l'articolo 17[322] o basando invece il suo giudizio sul combinato disposto tra articolo 17 e articolo 10.2[323].

Un simile utilizzo da parte dei giudici di Strasburgo della "clausola anti-abuso" non è però esente da critiche; un suo uso frequente può portare alla repressione di legittime voci di critica e minoritarie rispetto all'ideologia dominante. Questo è un rischio ancora maggiore nel contesto cibernetico, nel quale Internet pone in contatto persone provenienti da diversi contesti socio-culturali e appartenenti a differenti ordinamenti giuridici, dove quindi la libera espressione assume non assume connotati univoci, ma bensì mutevoli nelle diverse circostanze.

La diffusione globale delle reti digitali ha infatti evidenziato ancora di più l'impellente necessità di un approccio uniforme a livello internazionale in merito alla tutela della libertà di parola. La protezione pressoché assoluta garantita al *free speech* da parte del Primo Emendamento[324] della Costituzione americana deve infatti trovare un

---

[320] J.B.MIR, M.BASSINI, *op.cit.*

[321] H.CANNIE, D.VOORHOOF, *The abuse clause and freedom of expression in the European Human Rights Convention,* in *Netherlands Quarterly of Human Rights,* n.29, 2001, pp. 54-58.

[322] Corte EDU, sent. 7 luglio 2003, ricorso 65831/01, *Roger Garaudy c. Francia.*

[323] Corte EDU, sent. 23 settembre 1998, ricorso 24662/94, *Lehideux et Isorni c. Francia.*

[324] Il testo del Primo Emendamento alla Costituzione americana recita: "*Il Congresso non promulgherà leggi per il riconoscimento ufficiale di una religione, o che ne proibiscano la libera professione; o che limitino la libertà di parola, o di stampa; o il diritto delle persone di riunirsi pacificamente in assemblea e di fare petizioni al governo per la riparazione dei torti"*. La norma in questione assicura ai cittadini statunitensi una libertà *dallo* Stato, piuttosto che *nello* Stato. L'intento dei costituenti americani era quello di limitare le possibili ingerenze dei pubblici poteri in merito alle libertà fondamentali dell'essere umano entro limiti molto stretti e sostanzialmente invalicabili; la libertà di espressione non fa eccezione rispetto a questa realtà dei fatti.

punto di equilibrio con gli standard europei di cui si è appena data menzione. Questo possibile conflitto è stato alla base di numerosi procedimenti giurisdizionali nel corso degli ultimi anni da entrambe le sponde dell'Atlantico, sollevando numerose questioni in merito a conflitti di legge e scelta del foro competente[325]; la serie di pronunce in merito alla controversia *Yahoo! c. Licra*[326] ne è un valido esempio. I gestori del motore di ricerca *Yahoo!*, con sede legale negli Stati Uniti, avevano ricevuto l'ordine da un tribunale francese di bloccare l'accesso a un determinato sito Internet che vendeva materiale storico e accessori del regime nazista. I responsabili del *provider* avevano però rifiutato di adeguarsi a tale provvedimento, asserendo che i giudici francesi non avevano alcuna giurisdizione sul territorio degli Stati Uniti, aggiungendo inoltre che il blocco di un portale *web* si sarebbe configurato come un'inaccettabile infrazione al Primo Emendamento della Costituzione americana. Una successiva pronuncia di una Corte di Appello statunitense ha confermato la legittimità della sentenza emessa dal tribunale francese.

I giudici di Strasburgo si sono successivamente trovati a dover applicare questi criteri al contesto cibernetico, come testimoniato della pronuncia *Sunday Times c. Regno Unito*[327]. Secondo le parole della Corte EDU, la natura e le modalità delle possibili ingerenze statali nella libertà di espressione dipendono anche dal mezzo di comunicazione effettivamente utilizzato e dalle conseguenze che il suo utilizzo può avere nella società in termini di diffusione dell'informazione e reazione degli altri membri della collettività. Un particolare contenuto, suscettibile di immediata censura se condiviso attraverso i tradizionali *mass media*, potrebbe essere invece ritenuto legittimo se pubblicato su un sito Internet. Le particolari caratteristiche del *web* rendono inoltre assai complesso, se non impossibile, ostacolare in maniera efficace la diffusione di una determinata informazione sulla rete informatica. Il carattere transfrontaliero di Internet e la sua natura diffusa permettono infatti agli utenti di appoggiarsi a *server* situati in territorio estero rispetto al Paese intenzionato ad adottare provvedimenti di censura per continuare la loro opera di condivisione di informazioni.

---

[325] O.POLLICINO, M.BASSINI, *The law of the Internet: between globalisation and localisation*, in (a cura di) M.MADURO, K.TUORI, S.SANKARI, *Transnational law: rethinking European law and legal thinking*, Cambridge, 2014, pp.346 ss.

[326] Tribunal de Grande Instance de Paris, sent. 22 maggio 2000; United States Court of Appeal, 9th Circuit, sent. 12 gennaio 2006, *Yahoo! Inc c.Licra & UEJF*, 433 F3d 1199.

[327] Corte EDU, sent. 26 aprile 1979, ricorso n. 6538/76, *Sunday Times c. Regno Unito.*

La legittimità delle azioni volte a oscurare determinati siti Internet nonché il più generale problema del libero accesso allo spazio cibernetico sono gli argomenti al centro di uno dei più celebri casi affrontati dalla Corte EDU in materia di libera espressione nel *web*: *Yildirim c. Turchia*[328].

I fatti di causa hanno avuto ad oggetto la legittimità di un ordine restrittivo emanato da un tribunale turco volto a chiudere un sito Internet accusato di diffondere materiale ingiurioso nei confronti dell'eroe nazionale Atatürk. Il blocco non si limitava però ad impedire l'accesso al singolo portale incriminato, ma si estendeva a ogni indirizzo informatico consultabile attraverso il motore di ricerca *Google*. Di fronte a questa situazione, un accademico turco ha chiamato in giudizio il proprio Paese, poiché si era visto chiudere il proprio sito *web* senza alcuna apparente ragione, non avendo alcuna relazione con il materiale offensivo a cui si accennava poc'anzi. La Corte EDU ha dichiarato il blocco imposto dalle autorità turche illegittimo, in quanto non conforme ai principi di proporzionalità e necessarietà rispetto agli scopi perseguiti e privo di un effettivo fondamento nella normativa nazionale.

Un ulteriore tema affrontato dai giudici di Strasburgo è quello relativo alle caratteristiche e ai limiti effettivi della responsabilità dei *provider* in merito ai contenuti diffusi attraverso i portali informatici da loro gestiti: la sentenza *Delfi* ha affrontato proprio questa problematica[329].

Un celebre sito estone di informazioni giornalistiche permetteva ai propri utenti di pubblicare le proprie opinioni in merito alle notizie riportate senza che questi venissero in alcun modo filtrati o regolati in maniera preventiva. A corredo di un *reportage* giornalistico sui disservizi di una compagnia di trasporti, molti internauti si erano scagliati con commenti offensivi conto uno dei dirigenti di tale compagnia. Nonostante il fatto che tali ingiurie fossero state prontamente oscurate, la vittima di tali offese aveva intentato causa ai gestori del sito.

La Corte EDU, chiamata a giudicare sul caso in questione, non ha ravvisato alcuna violazione di quanto disposto dall'art.10 CEDU per diversi motivi. I responsabili del portale informatico avrebbero dovuto prevedere la possibile natura offensiva dei commenti e avrebbero quindi dovuto adottare le necessarie misure tecniche volte a prevenire la diffusione dei contenuti offensivi. I giudici hanno inoltre sottolineato che è

[328] Corte EDU, sent. 18 dicembre 2012, ricorso n. 3111/10, *Ahmet Yildirim c. Turchia.*
[329] Corte EDU, sent. 10 ottobre 2013, ricorso n. 64569/09, *Delfi AS c. Estonia.*

stata una precisa scelta editoriale dei gestori di permettere anche a utenti non registrati di pubblicare liberamente nella sezione commenti.

La sentenza *Delfi* non è esente da critiche sotto diversi aspetti; vengono applicati a contenuti liberamente condivisi da utenti informatici i criteri tradizionali di responsabilità editoriale. Non è possibile paragonare una simile situazione con, ad esempio, la scelta delle lettere dei lettori da pubblicare su un giornale cartaceo. Un ulteriore rischio è quello di attribuire un enorme potere di censura in capo ai gestori dei siti Internet, che rimarranno gli ultimi giudici a decidere cosa può essere pubblicato e condiviso in rete e cosa no.

Le criticità della pronuncia appena esaminata emergono chiaramente se si considera la posizione assunta dalla Corte EDU pochi mesi dopo nel caso *MTE*[330]. I giudici di Strasburgo, pur trovandosi a dover giudicare una situazione che presentava numerose somiglianze con quella alla base del caso *Delfi*, si sono pronunciati in maniera opposta rispetto alla loro precedente posizione. Secondo la Corte EDU, l'elemento di differenza era dato dal diverso valore diffamatorio dei commenti pubblicati *online*; in questo secondo episodio i giudici hanno infatti ravvisato una violazione della libertà di espressione ai sensi dell'art.10 poiché i contenuti oggetto di controversia non sono stati valutati così lesivi da meritarne l'immediata rimozione.

I giudici di Strasburgo hanno proseguito il loro ragionamento in merito alle effettive responsabilità di un gestore di siti internet nei confronti del comportamento dei propri utenti con la sentenza *Pihl*[331]. Oggetto di controversia è ancora una volta il punto di equilibrio tra tutela dei diritti alla personalità del singolo individuo e la libertà di espressione in ambito cibernetico. Riprendendo quanto già affermato nella sentenza *MTE*, la Corte EDU si è affidata a specifici criteri per valutare il caso concreto: la natura e il contenuto dei commenti offensivi postati nel sito Internet, il comportamento tenuto dai *provider* per limitare la diffusione del materiale controverso, l'effettiva responsabilità dell'autore di suddetti commenti in alternativa a quella del gestore del sito. Alla luce di queste linee guida, i giudici ritengono di poter limitare la libertà di espressione per tutelare la personalità del singolo soggetto solamente in caso di una lesione di particolare gravità all'immagine e alla reputazione della persona coinvolta, *rectius* in presenza di contenuti discriminatori e inneggianti all'odio e alla violenza. Occorre poi tenere in considerazione il comportamento tenuto dall'intermediario, segnatamente il gestore del sito, nel caso

[330] Corte EDU, sent. 2 febbraio 2016, ricorso 22947/13, *MTE c.Ungheria*
[331] Corte EDU, sent. 9 marzo 2017, ricorso 74742/14, *Pihl c.Svezia*.

concreto, ossia se abbia provveduto a rimuovere tempestivamente il contenuto oggetto di controversia una volta venutone a conoscenza.

La successiva pronuncia *Tamiz*[332] si colloca sulla medesima linea di condotta; anche in questo caso il gestore del sito Internet viene considerato responsabile solamente in presenza di commenti dall'alto contenuto offensivo e lesivo della reputazione delle persone contro il quale sono rivolti e in caso di ingiustificato ritardo nel rimuoverli.

La giurisprudenza fin qui esaminata ci permette di avanzare alcune riflessioni conclusive in merito all'atteggiamento tenuto dai giudici di Strasburgo nei confronti della problematica della libera espressione nel campo cibernetico[333]. La Corte EDU sembra considerare il mondo cibernetico come strettamente collegato alla realtà fisica concreta, e non come qualcosa di separato a sé stante. Questo porta i giudici ad applicare le tradizionali categorie giuridiche anche alle circostanze virtuali; questa applicazione rischia però di diventare problematica, considerando le diverse caratteristiche del mondo informatico rispetto a quello "reale". Il diritto alla libera espressione, parimenti a quanto succede per gli altri principi elencati nella CEDU, non deve essere considerato come assoluto e può quindi subire delle limitazioni per tutelare altri diritti di pari valore. Alla luce di ciò, i giudici devono valutare il caso concreto per individuare le modalità attraverso le quali raggiungere un punto di equilibrio tra i diritti della personalità del singolo e il valore della libera espressione. Ponendo l'attenzione sul contesto cibernetico, i giudici hanno optato per una sostanziale deresponsabilizzazione del gestore di sito Internet per quanto concerne i contenuti possibilmente offensivi postati dai vari utenti virtuali. Il responsabile viene individuato nell'autore dei commenti lesivi della reputazione altrui e non nell'intermediario che li ha (inconsapevolmente) diffusi, a meno che non abbia tardato a rimuoverli una volta che ne fosse venuto a conoscenza.

Per avere un quadro quanto più possibile completo della risposta giurisprudenziale in merito alla salvaguardia del diritto alla libera espressione, può essere utile esporre brevemente alcune decisioni della Corte di giustizia dell'Unione europea a tal riguardo. In particolar modo i giudici del Lussemburgo hanno avuto modo di pronunciarsi in merito alle responsabilità delle piattaforme digitali e ai limiti giurisdizionali degli obblighi ad esse spettanti.

[332] Corte EDU, sent.19 settembre 2017, ricorso n.3877/14, *Tamiz* c. *Regno Unito*.
[333] J.B.MAR, M.BASSINI, *op.cit.*

Il caso *Bolagsupplysningen e Ilsjan*[334] ha visto la violazione dei diritti della personalità di una persona giuridica; a tal proposito la Corte ha deciso che il soggetto che si ritiene leso può avanzare una domanda di risarcimento del danno dinanzi ai giudici dello Stato membro dove ha il centro dei propri interessi oppure del Paese dove si è materialmente concretizzato il danno stesso, se diverso dal luogo della sede statutaria.

La natura diffusa e sovranazionale della rete Internet può comportare che un contenuto controverso venga diffuso su scala potenzialmente globale; la Corte ha quindi voluto impedire la parcellizzazione delle domande di risarcimento in una molteplicità indefinita di sedi giudiziarie. Si vuole porre quindi un freno alla tendenza del *forum shopping*.

La recente pronuncia *Glawischnig-Piesczek*[335] permette di fare una breve riflessione sui limiti del diritto alla cancellazione e sugli obblighi che questo solleva per i gli intermediari e i gestori di siti Internet. La Corte di giustizia ha infatti specificato che la persona interessata può richiedere la rimozione dei contenuti lesivi su base nazionale. Il *provider*/ intermediario è però tenuto a limitare l'accesso a tale materiale su scala globale, cancellando inoltre qualsiasi oggetto equivalente ai contenuti dichiarati lesivi. Questa ultima precisazione lascia qualche dubbio meritevole di menzione. Non viene infatti specificato cosa si intende per "equivalente", lasciando un grande margine di discrezionalità ai soggetti coinvolti; questo può causare prese di posizione lesive per la libertà di espressione, andando a limitare la diffusione di contenuti non meritevoli di censura.

I giudici della Corte di giustizia, parimenti ai loro colleghi di Strasburgo, si trovano a dover ragionare in un ambito caratterizzato da elementi sovranazionali e che quindi mettono a dura prova le tradizionali categorie giuridiche. In tali circostanze, devono trovare un punto di equilibrio tra interessi spesso contrapposti. L'unica soluzione possibile è valutare effettivamente il caso concreto, tenendo presente le peculiarità e gli strumenti tecnologici disponibili utilizzati dai gestori di piattaforme e dagli intermediari per evitare lesioni ai diritti della personalità dei soggetti coinvolti.

[334] Corte di giustizia dell'Unione europea, sent.17 ottobre 2017, causa C-194/16, *Bolagsupplysningen e Ilsjan c.Svensk Handel AB*, ECLI:EU:C:2017:766

[335] Corte di giustizia dell'Unione europea, sent.3 ottobre 2019, causa C-18/18, *Glawischnig-Piesczek c.Facebook Ireland*, ECLI:EU:C:2019:821.

5. Gli effetti collaterali della comunicazione nell'epoca digitale: il fenomeno della filter bubble e l'imperativo dello sharing

L'analisi della giurisprudenza in merito alla comunicazione via *web* permette di approfondire ulteriormente i meccanismi della condivisione di informazioni attraverso le reti digitali.

I motori di ricerca, così come i portali di informazione e di *social media*, utilizzano complessi procedimenti matematici chiamati algoritmi per individuare quali notizie fornire all'utente. Questi calcoli si basano sui dati ricavati dalla navigazione *on-line* del singolo internauta; attraverso un'attenta analisi delle sue abitudini virtuali, le aziende e gli ISP che utilizzano sistemi algoritmici possono offrire all'utente cibernetico un'esperienza di navigazione sempre personalizzata sulle sue esigenze.

L'utilizzo sempre maggiore degli algoritmi ha però un effetto secondario che non deve essere trascurato: la creazione di una *filter bubble*[336], ossia di una bolla costruita secondo i gusti, le preferenze e i pregiudizi dell'utente e nella quale quest'ultimo viene rinchiuso. L'algoritmo filtra le miriadi di informazioni presenti nel *cyberspace* proponendo all'internauta esclusivamente quelle che rispecchiano la sua personalità, rafforzandolo quindi nelle sue opinioni e nei suoi convincimenti, indipendentemente dalla veridicità di questi ultimi. L'utente si ritrova in una sorta di *echo chamber* in cui sente "rimbombare" esclusivamente i propri pensieri[337].

La personalizzazione dello spazio cibernetico non ha una connotazione esclusivamente negativa, ma varia a seconda delle circostanze. Un consumatore trae effettivo giovamento dal ricevere consigli e suggerimenti in merito ai possibili acquisti da fare, risparmiando così tempo e denaro. La situazione è differente per quanto riguarda il potenziale elettore: il dibattito politico è infatti vitale per una società democratica, così come la diffusione anche delle idee minoritarie e non allineate con la visione politica dominante[338]. La *filter bubble* non favorisce certo il confronto, facendo in modo che ogni persona rimanga ferma nelle sue convinzioni non accettando il dialogo con l'altro.

Un altro fenomeno a cui si deve prestare attenzione è il cd. *sharing*; l'idea della condivisione è alla base delle reti digitali, e in particolar modo dei *social network*[339]. Gli

[336] E.PARISIER, *Filter bubble: how the new personalized web is changing what we read and what we think*, New York, 2011, pp.13 ss.
[337] G. PITRUZZELLA, *op.cit.*
[338] C.R.SUNSTEIN, *Republic.com 2.0*, Princeton, 2007, pp.38 ss.
[339] G.PITRUZZELLA, *op.cit.*

utenti delle piattaforme sociali sono spinti a condividere materiali multimediali, così come a stringere relazioni e amicizie. Sono incentivati anche ad entrare in relazione con terze parti[340], direttamente esterne al portale sociale, ma che possono utilizzare questo ecosistema per diffondere notizie e contenuti. I rinvii e i *link* effettuati dai profili di utenti dei *social media* possono ampliare a dismisura la platea di lettori e fruitori di contenuti esterni alla piattaforma sociale, rendendoli cosi "virali" e fonti di grandi guadagni.

6. *La diffusione delle fake news. I possibili rimedi giuridici all'inquinamento del public discourse*

L'ambiente appena descritto è ideale per la diffusione e la proliferazione delle cd. *fake news.* Questo termine vuole indicare una notizia falsa o fuorviante diffusa in maniera intenzionale attraverso lo spazio cibernetico, allo scopo di influenzare in una determinata direzione l'opinione pubblica[341]. Ovviamente le false informazioni e i depistaggi non sono una novità dell'epoca digitale, ma hanno caratterizzato la vita sociale e politica per secoli. Si pensi a tal proposito alla Donazione di Costantino, ossia al documento apocrifo secondo il quale l'impero romano avrebbe acconsentito alla giurisdizione del papato sul territorio di Roma, dell'Italia e financo sull'intero Occidente. Questo atto funzionava quindi da legittimazione storico-politica al predominio della Chiesa sull'impero. La falsità di tale documento fu dimostrata dall'umanista Lorenzo Valla attraverso uno scritto pubblicato nel 1517.

In epoca ben più recente il *Sun*, un giornale di New York, ha pubblicato una serie di 6 articoli, partendo dal 25 agosto 1835, descrivendo la scoperta di una società civilizzata con base sulla Luna.

Un ulteriore esempio di notizia fasulla propagandata artificiosamente è data dal discorso pronunciato dal presidente statunitense Roosevelt la sera del 27 ottobre 1941[342], in cui si accusava falsamente la Germania nazista di preparare un attacco alle coste americane con i temibili sommergibili U-Boot. Queste parole fecero una grande presa

[340] J.VAN DIJCK, *The culture of connectivity*, Oxford, 2013, pp.46.
[341] Definizione di *fake news* fornita dall'enciclopedia Treccani, http://www.treccani.it/enciclopedia/fake-news/ (consultato il 27 settembre 2019).
[342] L'audio del discorso del presidente Roosevelt è consultabile al seguente link https://www.express.co.uk/news/world/1174437/WW2-news-hitler-map-nazi-propaganda-roosevelt (consultato il 27 settembre 1941).

sull'opinione pubblica statunitense, consentendo al presidente Roosevelt di ottenere il proprio *casus belli* per muovere guerra al Terzo Reich.

Come si è appena visto, le informazioni false non sono una prerogativa dell'epoca digitale, ma hanno certamente trovato nello spazio cibernetico un ambiente ideale per la propria diffusione per diverse ragioni. La struttura fortemente decentralizzata di Internet non permette alcun controllo preventivo da parte di una qualche autorità sull'effettiva autorevolezza e veridicità dei contenuti diffusi in rete. I meccanismi di controllo applicati dai giornali *on-line* per garantire l'autenticità delle informazioni condivise attraverso i loro portali non trova applicazione per quanto riguarda i *blog* o siti privati, che possono quindi diffondere *fake news* senza timore alcuno di eventuali ritorsioni.

L'elemento dello *sharing* a cui si faceva riferimento poc'anzi è un'altra causa della proliferazione delle notizie fasulle. Gli utenti dei *social media*, attraverso *retweet*, *like* e condivisioni, contribuiscono ad aumentare a dismisura la platea di potenziali lettori delle *fake news.*

Il fenomeno dell'*echo chamber* crea inoltre un pubblico di lettori di notizie sempre più polarizzato e frammentato, convinto delle proprie opinioni e restio al confronto con altri pensieri e ideologie diverse dalla propria.

La rapida diffusione delle *fake news* è favorita anche dalla scarsa, per non dire inesistente, regolamentazione delle piattaforme sociali: pur non essendo strettamente catalogabili come mezzi di informazione, i *social network* sono luoghi virtuali in cui le notizie circolano e si propagano. L'Unione europea ha riconosciuto il pericolo per la corretta formazione della coscienza pubblica insito nella proliferazione delle notizie fasulle attraverso i *social media*, chiedendo ai gestori di tali siti di intervenire attivamente per contrastare questo fenomeno[343]. Il Consiglio di Europa si è espresso su simili toni, auspicando un maggiore impegno dei Paesi membri nella regolamentazione del mondo *on-line*, anche attraverso una stretta cooperazione tra gestori delle piattaforme sociali e pubblici poteri[344].

[343] D.BOND, D.ROBINSON, *European Commission fires warning at Facebook over fake news*, in *Financial Times*, 30 gennaio 2017, https://www.ft.com/content/85683e08-e4a9-11e6-9645-c9357a75844a (consultato il 28 settembre 2019).
[344] Consiglio di Europa, risoluzione 2143, 25 gennaio 2017, *Online media and journalism: challenges and accountability.*

Gli attuali strumenti giuridici rendono però assai ardua la lotta alle *fake news*, e specialmente alla loro diffusione attraverso i *social media*[345]; la rettifica, o addirittura la censura, di una determinata notizia diffusa via *web* non raggiungerebbe infatti tutte le persone che hanno consultato la versione precedente di detta informazione. L'aggiornamento della notizia si avrebbe inoltre sulla versione diffusa dal sito di origine e non su quella condivisa sul *social network*. In altre parole, i tradizionali sistemi giuridici utilizzati per garantire l'autenticità delle notizie diffuse a mezzo stampa rischiano di essere inefficaci nel contesto cibernetico.

Al fine di arginare la diffusione delle notizie fasulle attraverso i *social media* e di preservare così la libera formazione dell'opinione pubblica, occorre coinvolgere in prima persona i gestori delle piattaforme sociali; solamente loro hanno la possibilità di intervenire in maniera diretta e tempestiva sui contenuti diffusi attraverso i loro *network*. Questa possibile soluzione solleva però nuove problematiche meritevoli di un'attenta considerazione: quali rischi comporta incaricare una società privata e con nessun legame con l'autorità pubblica di decidere in maniera autonoma quali contenuti meritano la diffusione e quali invece devono cadere nell'oblio?

Facebook ha approntato uno specifico sistema per limitare la condivisione delle *fake news*: ogni utente iscritto al famoso *social network* può segnalare una particolare notizia ritenuta falsa o fuorviante. Questa segnalazione porta a un successivo controllo effettuato con un *fact checking* di confronto con quanto riportato sul fatto controverso dalle più famose e autorevoli agenzie di stampa. Qualora l'informazione segnalata risultasse falsa in seguito a tale controllo, verrebbe poi cancellata e oscurata dai responsabili del *social network.*

Questo sistema di prevenzione per la diffusione delle *fake news* presta però il fianco a specifiche critiche[346]. *In primis*, è caratterizzato da un'intollerabile lentezza; la prima notizia falsa sottoposta al regime di controlli appena menzionato è stata censurata solamente dopo che aveva raggiunto le 81mila condivisioni su *Facebook*[347]. In secondo luogo, il meccanismo descritto funziona solo in ottica futura; i lettori che hanno già

[345] M.MONTI, *Fake news e social network: la verità ai tempi di Facebook,* in *Rivista del Diritto dei Media*, n.1, 2017, http://www.medialaws.eu/wp-content/uploads/2019/05/8.-Monti.pdf (consultato il 30 settembre 2019).
[346] M.MONTI, *ibidem.*
[347] B.RUFFILI, *Il sistema di verifica delle notizie false di Facebook arriverà presto anche in Italia*, in *La Stampa.it*, 5 marzo 2017, https://www.lastampa.it/tecnologia/news/2017/03/05/news/il-sistema-di-verifica-delle-notizie-false-di-facebook-arrivera-presto-anche-in-italia-1.34629804 (consultato il 30 settembre 2019).

consultato la notizia falsa non vengono informati del fatto che tale informazione è stata riscontrata come mendace. Non vengono perciò riparati i danni già causati dalla diffusione della *fake news*; si cerca solamente di impedire che ne vengano causati altri. Il problema principale, già precedentemente accennato, è quello relativo alla connotazione socio-politica dei controllori e del loro operato. L'ideologia dei tecnici adibiti al *check* delle *fake news* potrebbe certamente influire sulle loro azioni, così come eventuali direttive impartite dai gestori del *social network.* Questi sono i rischi insiti nel delegare tali funzioni di controllo a un'entità esclusivamente privata, che risponde solamente alle logiche del profitto e non ha alcun obbligo verso i cittadini; potrebbe essere perciò più opportuno un diretto intervento dei pubblici poteri nella regolamentazione dell'azione dei *social network*, al fine di mantenere al sicuro lo svolgimento del *public discourse* e di garantire la libera espressione per gli utenti cibernetici.

6.1. Il report della Commissione europea sulle fake news

Il problema relativo alla proliferazione delle *fake news* nell'ambiente cibernetico e al conseguente inquinamento del processo di formazione dell'opinione pubblica è al centro del dibattito europeo. Un gruppo di esperti, selezionati dalla Commissione europea in maniera tale da affrontare il tema delle *fake news* in un'ottica multidisciplinare, ha prodotto un report sull'argomento di cui vale la pena dare menzione[348]. Questo documento propone una serie di *best practice* da far adottare agli attori coinvolti nel sistema virtuale, stimolando una proficua collaborazione tra soggetti privati ed enti pubblici per arginare il fenomeno delle notizie fasulle. Il report fornisce inoltre numerosi spunti di riflessioni utili per il presente studio, anche in campo linguistico-terminologico. Si sottolinea infatti che il termine *fake news* può non descrivere in maniera adeguata il fenomeno in questione. Si assiste spesso a procedure organizzate su ampia scala di disturbo del dibattito pubblico, utilizzando raffinati strumenti tecnologici come *account* automatizzati e *bot* programmati per diffondere fandonie e maldicenze. Simili sistemi richiedono un'attenta pianificazione e corposi investimenti in termini di risorse economiche; non si parla di semplice diffusione di notizie fasulle, ma di attacchi organizzati alla libera formazione dell'opinione pubblica. Gli esperti suggeriscono di

[348] Commissione europea, *Final Report of the High Level Expert Group on Fake News and Online Disinformation*, 12 marzo 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation (consultato il 30 settembre 2019).

adottare delle procedure trasparenti per combattere la diffusione delle notizie fasulle che vedano la collaborazione sia dello Stato che dei soggetti privati coinvolti nel mondo cibernetico.

7. Riflessioni conclusive

L'avvento delle nuove tecnologie di comunicazione, e in particolar modo di Internet, ha radicalmente trasformato il tradizionale meccanismo dell'informazione. Le categorie giuridiche ideate per regolamentare il diritto alla libera espressione fanno riferimento a un'epoca in cui lo spazio cibernetico era un concetto pressoché fantascientifico. Occorre perciò chiedersi se possono ancora essere attuali ed efficaci nel contesto virtuale od occorre invece riformularle alla luce dei cambiamenti apportati dal progresso tecnologico.

Il presente capitolo ha voluto mettere in luce quanto stretto sia il legame tra diritto all'informazione e libertà di parola, specialmente nell'epoca digitale; la diffusione dei *device* informatici a un prezzo relativamente contenuto e la connettività Internet che ha ormai raggiunto una dimensione globale hanno reso ogni utente un potenziale produttore di informazioni, scardinando il predominio dei *mass media* tradizionali. Ogni persona può quindi far sentire la propria voce nell'etere informatico e diffondere le informazioni di cui è in possesso.

Una simile situazione non era certamente immaginabile quando il diritto alla libera espressione è stato riconosciuto ed enunciato nei diversi trattati internazionali di cui si è dato conto in queste pagine.

Strumenti come i *social media* funzionano oggi come importante cassa di risonanza per i contenuti che vengono condivisi su queste piattaforme; siti come *Facebook* o *Twitter*, pur non producendo informazioni in maniera diretta, contribuiscono alla loro diffusione. La sfida principale da affrontare a livello politico e legislativo è proprio quella di inquadrare in una maniera giuridicamente corretta la natura di questi portali di *social media*, anche alla luce del loro operato e dell'importanza che ormai rivestono nella formazione dell'opinione pubblica. Pur avendo una natura privata e votata al profitto economico, influenzano la coscienza politica della collettività con una forza mai raggiunta prima da altri mezzi di comunicazione. Sono infatti i gestori di tali piattaforme sociali a decidere quali contenuti possono essere diffusi e quali invece devono essere censurati: il diritto alla libera espressione nel mondo digitale rischia di essere

esercitato solamente attraverso l'operato dei presidenti dei consigli di amministrazione di Twitter o Facebook.

Si suggerisce un intervento legislativo, perlomeno a livello europeo, volto a riconoscere e formalizzare l'azione dei *social media* nel campo politico ed elettorale, seguito poi da una stretta collaborazione tra i gestori di tali siti e i governi nazionali per trovare modalità efficaci con cui combattere fenomeni odiosi e deleteri come le *fake news* o i discorsi di incitamento all'odio.

Un primo sviluppo in tal senso può essere il Codice di condotta[349] per combattere l'*hate speech*, pubblicato dall'Unione europea nel giugno 2016.

Si tratta di un accordo volontario con cui i più grandi operatori nel settore delle informazioni *on-line* (segnatamente Facebook, Microsoft, Twitter, YouTube. Nel 2018 si sono aggiunti Instagram, Snapchat, Dailymotion, e nel 2019 Jeuxvideo.com) accettano di prendere le misure necessarie per difendere la libera espressione nello spazio cibernetico e per impedire la diffusione di materiale d'odio attraverso la rete. I gestori di queste piattaforme informatiche si sono impegnati a fornire ai propri utenti gli strumenti necessari per segnalare qualsiasi comportamento scorretto che violi le linee guida sottoscritte al momento dell'iscrizione a detti portali e, ove applicabili, le leggi nazionali. In seguito a tale segnalazione, saranno gli stessi gestori a valutare se il contenuto segnalato sia in violazione delle regole accettate dagli utenti.

Fare riferimento a termini di utilizzo specifici per ogni singola piattaforma può rendere però l'esercizio della libera espressione difforme e disomogeneo: a mero titolo di esempio, un contenuto ritenuto inaccettabile per YouTube può superare il controllo di Twitter. Occorre inoltre tenere in considerazione le diverse percezioni culturali; la libertà di parola è un valore da contemperare con altri interessi e diritti in Europa, mentre ha una valenza più assoluta negli Stati Uniti[350].

I responsabili delle piattaforme stanno gradualmente assumendo sempre più il ruolo di "controllori" del *public discourse* in Internet, controllando quali contenuti possano essere diffusi e quali invece bloccati, proponendo standard spesso più severi rispetto a quelli prefissati dalla legge[351].

---

[349] The EU Code of conduct on countering illegal hate speech online, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en (consultato il 22 gennaio 2020).

[350] P.CAVALIERE, *Digital platforms and the rise of global regulation of hate speech*, in *Cambridge International Law Journal*, vol.8 (2019) Issue 2, pp.282-304.

[351] P.CAVALIERE, *ibidem.*

La "privatizzazione" della libera espressione, intendendosi con tale termine l'assegnazione a soggetti privati della decisione in merito a cosa è meritevole di diffusione e cosa invece di censura, rischia di avere effetti potenzialmente dannosi.

In primis, una mancanza di trasparenza in merito ai criteri utilizzati per prendere tali decisioni e una precaria tutela giurisdizionale della libera espressione per gli utenti cibernetici, dato che è spesso complesso individuare le procedure da adottare e i soggetti a cui rivolgersi per far sì che un sito o un contenuto "oscurato" possa tornare *on-line*.

Il ruolo sempre più importante delle piattaforme digitali nella definizione degli standard informatici di espressione e libertà di parola può rappresentare il punto principale di un nuovo modello di autotutela che si affianca, per quanto riguarda il mondo cibernetico, alla tradizionale giurisdizione statale[352].

Questo però non deve significare la retrocessione dello Stato a un ruolo di mero spettatore; i soggetti privati agiscono infatti in una legittima ottica di profitto e senza dover rispondere alla cittadinanza. Considerato ciò, la circolazione delle informazioni potrebbe risultare inquinata da interessi economici, con conseguente detrimento dell'esercizio della libera espressione. Si auspica perciò una supervisione statale sull'operato delle piattaforme per preservare un corretto esercizio della libertà di parola.

L'esempio del Codice di condotta contro il discorso di odio appena menzionato permette di svolgere alcune riflessioni ulteriori in merito alla possibile delega a soggetti privati di compiti di censura digitale.

I primi report sul funzionamento del Codice stesso[353] testimoniano una grande divergenza a livello applicativo nei vari Stati membri: questo è giustificato dalle differenze a livello di previsioni normative nazionali. Un determinato contenuto può essere considerato illecito in uno Stato e accettabile in un altro: questa situazione rende assai complesso, e dotato di un certo margine di discrezionalità, il lavoro dei revisori incaricati da parte delle compagnie private firmatarie del codice. A mero titolo di esempio, uno studio commissionato dalla Commissione europea certifica che solo due Paesi membri sanzionano a livello penale l'odio razziale per il colore della pelle[354].

---

[352] P.CAVALIERE, *ibidem.*

[353] B.SAETTA, *Codice europeo contro l'hate speech: i primi risultati e cosa non va,* https://www.valigiablu.it/codice-europeo-hate-speech/ (consultato il 24 aprile 2020).

[354] Mandola Project: monitoring and detecting online hate speech, http://mandola-project.eu/m/filer_public/7b/8f/7b8f3f88-2270-47ed-8791-8fbfb320b755/mandola-d21.pdf (consultato il 24 aprile 2020).

Risulta evidente la mancanza di un approccio unitario a livello di diritto dell'Unione europea: non c'è una definizione normativa unitaria di *hate speech* e, di conseguenza, non c'è un elenco di quali comportamenti rientrino in tale categoria.

Una simile situazione rischia di assicurare un potere di censura potenzialmente indefinito nei suoi limiti alle *corporation* dello spazio cibernetico con conseguente pericolo per i diritti fondamentali degli utenti. Pur auspicando un intervento legislativo in materia, si possono proporre alcuni correttivi al Codice per garantire una maggiore trasparenza. Un elenco delle decisioni di rimozioni di contenuti e delle motivazioni che ne stanno alla base e, di conseguenza, la possibilità per i soggetti coinvolti di poter ricorrere in sede giurisdizionale contro tali azioni potrebbero essere i primi passi da compiere[355].

Capitolo 4

La privacy nell'epoca digitale: un bilanciamento tra interessi contrapposti per un'efficace tutela giurisdizionale e normativa del diritto alla riservatezza e all'autonomia informativa

Sommario: Introduzione. - 1. L'evoluzione storico-culturale del concetto di privacy. - 1.1. Una breve storia dell'idea di privacy: dalla vergogna biblica all'autonomia informativa. - 1.2. L'idea di privacy nei diversi contesti sociali e geografici. - 1.2.1. L'idea di privacy nella cultura africana: dal pensiero collettivo della filosofia Ubuntu all'individualismo moderno. - 2. Una definizione giuridico-filosofica di privacy nel contesto cibernetico: il diritto all'habeas data. - 2.1. Le reti digitali e le sfide per l'autonomia personale nello spazio cibernetico. - 2.1.1. Il consenso al trattamento dei dati personali nel contesto cibernetico può dirsi effettivamente libero e informato? - 3. La privacy come diritto fondamentale nel contesto cibernetico. - 3.1. Il diritto all'autonomia informativa come prerogativa della persona. - 4. I principali strumenti legislativi internazionali a tutela del diritto alla protezione dei dati personali. - 4.1. Il diritto all'autonomia informativa nel quadro giuridico delle Nazioni Unite. - 4.2. Il diritto alla privacy nell'art.8 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali. - 4.2.1. La definizione di "vita privata" e il diritto alla protezione dei dati personali nella giurisprudenza della Corte Europea dei Diritti dell'Uomo. - 4.3. La

[355] B.SAETTA, *ibidem.*

Convenzione 108 del Consiglio di Europa: il primo documento internazionale in materia di trattamento automatico dei dati. - 4.4. Il diritto alla privacy e all'autonomia informativa nell'ordinamento dell'Unione europea. - 4.5. Il diritto alla tutela dei dati personali nei Trattati istitutivi dell'Unione europea. - 4.6. Dalla direttiva 95/46/CE al Regolamento (UE) 2016/679: l'evoluzione normativa europea nella tutela dei dati personali. - 5. Il Regolamento (UE) 2016/679 (GDPR) e la tutela dei dati personali nell'epoca digitale. - 5.1. La definizione di "dato personale" fornita dal Regolamento (UE) 2016/679. - 5.2. Trattamento, profilazione e pseudonimizzazione: la raccolta e la gestione dei dati personali secondo il Regolamento (UE) 2016/679. - 5.3. I criteri di applicazione materiale e territoriale del Regolamento 2016/679 e i profili innovativi rispetto alla normativa previgente. - 5.4. Privacy by design e Privacy by default: il Regolamento (UE) 2016/679 introduce due nuovi approcci alla protezione dei dati personali. - 5.5. I diritti garantiti all'interessato dal Regolamento (UE) 2016/679. - 5.5.1. L'interconnessione globale e il diritto alla portabilità dei dati. - 5.5.2. L'evoluzione del diritto all'oblio e la sua disciplina all'interno del Regolamento (UE) 2016/679. - 5.5.3. Il diritto all'accesso ai propri dati personali nel Regolamento (UE) 2016/679 come prerogativa per l'esercizio dell'autonomia informativa. - 5.6. Il trasferimento dati fuori dai confini europei sotto l'egida del Regolamento (UE) 2016/679. - 6. Il Regolamento (UE) 2016/679 come nuovo standard globale in termini di tutela dell'autonomia informativa e di data protection.

Introduzione

"On the Internet, nobody knows you're a dog."

"*Nell' Internet nessuno sa che sei un cane"*. La celebre vignetta[356] pubblicata sulla rivista *New Yorker* riassume in poche parole una delle peculiarità che, teoricamente, dovrebbe caratterizzare lo spazio cibernetico: l'anonimato, e con esso la privacy digitale. La struttura diffusa della rete Internet, priva di un qualsiasi controllo centralizzato e accessibile a qualunque soggetto in possesso dei mezzi tecnologici necessari, dovrebbe permettere la navigazione del *cyberspace* senza dover rivelare la propria identità.

La realtà è però ben diversa; non solo è possibile scoprire se l'utente è un cane, ma anche la sua razza, che tipo di croccantini preferisce e quale gatto ha inseguito il giorno prima[357].

Il costante sviluppo tecnologico ha infatti portato ad una situazione apparentemente paradossale: gli stessi strumenti utilizzati per preservare l'anonimato nel contesto cibernetico possono essere parimenti adoperati per ridurre e intaccare la sfera di riservatezza e intimità del singolo utente informatico. Prendere parte alla vita digitale comporta esporre la propria privacy a rischi non indifferenti[358]. La tecnologia permette di raccogliere informazioni in tempo reale, di condividerle e renderle accessibili a qualunque

[356] Vignetta realizzata da P.STEINER e pubblicata sulla rivista *New Yorker* il 5 luglio 1993, https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html (consultato il 4 luglio 2019).
[357] P.BERNAL, *Internet Privacy Rights. Rights to protect autonomy*, New York, 2014, pp.53.
[358] A.SAVIN, *EU Internet Law*, Cheltenham, 2014, pp. 191 e ss.

soggetto connesso alla rete informatica. I dati personali sono diventati merce di scambio tra società e imprese che utilizzano tali informazioni per scopi commerciali, proponendo beni e servizi realizzati secondo le aspettative e i desideri del potenziale cliente. Il prezzo per partecipare all'*agorà* digitale, pena l'esclusione dalla vita sociale, è la condivisione dei propri dati personali; navigando in Internet e interagendo con i *social network* gli utenti rivelano i propri pensieri, i propri gusti e le proprie attività.

Non è certamente una novità dell'epoca attuale la raccolta informazioni personali e il loro utilizzo per i più diversi scopi. Il fattore che espone la privacy degli utenti digitali a rischi mai riscontrati prima è la possibilità di mettere in relazione i dati raccolti grazie all'incremento della velocità di calcolo dei moderni *device* informatici e alla loro relativa economicità[359]. Ad esempio, inserire un indirizzo o un numero di telefono in un comune motore di ricerca informatico può portare a scoprire ulteriori informazioni riferite al soggetto in esame, come il nome, l'età, la provenienza geografica o altro ancora.

Sono quindi numerose le occasioni e gli ambiti in cui il diritto alla privacy può subire minacce nel contesto digitale, proprio per la crescente importanza che le nuove tecnologie stanno acquisendo nella vita quotidiana. Il mondo cibernetico è ormai interconnesso con la realtà fisica concreta; i dati raccolti *on-line* non possono essere separati e gestiti in maniera autonoma da quelli raccolti *off-line.* L'esigenza di un'efficace tutela del diritto alla privacy è perciò quanto mai attuale ai giorni nostri, ma tale necessità solleva ulteriori questioni preliminari sull'effettiva natura dello spazio cibernetico[360].
Per poter accedere a questa dimensione virtuale, occorre il coinvolgimento sia di attori di provenienza pubblica che privata; sono infatti necessarie strumentazioni fornite dagli Stati, come i cavi elettrici, ma anche quelle fornite da industrie private come *server e router*. La maggior parte dei siti *web* sono inoltre condotti e gestiti da soggetti privati. Considerato ciò, il *cyberspace* deve essere considerato uno spazio pubblico o è invece una realtà privata? La risposta a questa domanda non soddisfa un mero interesse accademico, ma comporta importanti conseguenze giuridiche. Se si vuole aderire alla seconda opzione prospettata, si deve di conseguenza affermare che le regole di condotta e di gestione di Internet non devono essere formulate dallo Stato, ma dal gestore del singolo sito. Nel caso opposto, spetta invece al potere pubblico promulgare norme adeguate a regolamentare la vita digitale, come è effettivamente accaduto nel corso degli anni e a diversi livelli. Lo spazio cibernetico è stato perciò considerato come una realtà

[359] A.SAVIN ,*ibidem.*
[360] P.BERNAL, *op.cit.*, pp.7 ss.

pubblica, suscettibile di essere sottoposta alla legislazione statale. La conseguenza di ciò è che i diritti riconosciuti dallo Stato nel mondo fisico, trovano spazio anche nel contesto cibernetico; il cittadino deve essere infatti adeguatamente tutelato durante la sua navigazione nel *web*.

Questo però porta a una contraddizione, che si rivela però solo apparente. Come può esistere un diritto alla riservatezza, e quindi ad una sfera privata, in uno spazio pubblico, come si è detto essere il *cyberspace?*

La pervasività della rete Internet ha radicalmente cambiato la prospettiva umana; ogni persona vive infatti continuamente connessa a un grande *network* di comunicazioni attraverso il quale condivide in maniera continua informazioni. La possibilità di registrare ogni movimento, di condividere ogni pensiero o stato d'animo attraverso la rete informatica fa sì che la trasparenza sia l'elemento caratterizzante di questa epoca, contribuendo alla dissoluzione del confine tra sfera privata e pubblica[361].Una simile realtà dei fatti comporta la riduzione dei rispettivi spazi privati, provocando la moltiplicazione degli appelli alla privacy e la consapevolezza della necessaria evoluzione di questo concetto, al fine di adattarlo alle nuove e mutate esigenze della società attuale[362].

Uno degli obbiettivi principali del presente studio è proprio quello di analizzare l'evoluzione dell'idea stessa di privacy nel contesto digitale, individuando principi e valori riferibili al lungo periodo che possono rimanere validi a prescindere dall'avanzamento delle nuove tecnologie, senza necessitare quindi di una continua riforma normativa. I suddetti principi devono tener conto dei contrapposti interessi in gioco[363]. Soggetti come gli individui, i governi e le aziende esprimono infatti esigenze e preoccupazioni diverse. I primi hanno la necessità di mantenere la propria autonomia e individualità; tale bisogno può essere ostacolato dall'interesse dei pubblici poteri di mantenere la sicurezza all'interno dei propri confini attraverso operazioni di sorveglianza e di raccolta dati. Non bisogna poi trascurare l'attività delle grandi società imprenditoriali che hanno un continuo bisogno di informazioni relative ai potenziali clienti per fornire beni e servizi sempre più redditizi e incrementare così i loro guadagni. Trovare un punto di equilibrio si rivela fondamentale per esprimere efficacemente la funzione del diritto alla privacy nel contesto cibernetico; chiarito tale punto, sarà molto più semplice

[361] J.DAMEN ET AL. *The human right of privacy in the digital age*, in *Staat, Recht und Politik — Forschungs- und Diskussionspapiere,* n.3, 2017, pp.1-11.
[362] S.RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, pp. 19 ss.
[363] P.BERNAL , *op.cit..*, pp.15 ss.

formulare leggi e regolamenti per venire incontro alle necessità degli utenti cibernetici in materia di riservatezza e autonomia informativa.

Per raggiungere questo obbiettivo, occorre riflettere sul concetto stesso di privacy, analizzando la sua evoluzione nel corso degli anni e le sue differenti interpretazioni condizionate dai diversi contesti culturali e geografici. Una volta chiaritene le caratteristiche principali, è possibile esaminare con cognizione di causa la definizione giuridica di diritto alla privacy; per fare ciò, è necessario studiare i trattati e le convenzioni internazionali che hanno riconosciuto il suddetto diritto, mettendone in risalto le similarità e le differenze. L'attenzione si sposta infine sul contesto normativo europeo e, in particolare, sul nuovo Regolamento in materia di protezione dei dati personali che si sta affermando come standard normativo globale di tutela. Il ruolo primario dell'Unione europea nell'economia mondiale e la natura di Internet come rete senza confini politici e giuridici sono solo alcuni degli elementi che stanno portando i legislatori extra-europei e le corti internazionali a riconoscere al Regolamento (UE) 2016/679 (GDPR)[364] una valenza non limitata solamente al territorio dell'Unione, seppur con alcune particolarità e distinzioni, come si andrà a vedere successivamente. Un ulteriore quesito a cui vuole rispondere il presente studio è se davvero la nuova normativa europea può affermarsi come livello di tutela minima richiesta per il diritto alla privacy e all'autonomia informativa nel contesto digitale.

1. L'evoluzione storico-culturale del concetto di privacy

Uno spazio autonomo, libero da ingerenze esterne, è un requisito fondamentale per il corretto sviluppo di una personalità indipendente. Avere a disposizione un ambiente dove affermare la propria opinione ed esprimere le proprie idee senza dover fornire alcuna giustificazione e senza dover temere il giudizio altrui è una necessità avvertita da ogni persona. L'identità personale non può prescindere dal rispetto della privacy[365]. Le nuove tecnologie rischiano di limitare la sfera decisionale delle persone attraverso il loro carattere pervasivo; gli annunci pubblicitari progettati in linea con i gusti del consumatore

[364] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in GU L 119, 4 maggio 2016, pp.1-88.

[365] B.PERINAN, *The origin of privacy as a legal value: a reflection on Roman and English law,* in *American Journal of Legal History,* vol.52, 2012, pp.183-201.

possono infatti far nascere in quest'ultimo il bisogno di acquistare quel determinato bene o di usufruire di quello specifico servizio. Gli spot elettorali diffusi attraverso il *web* che si focalizzano sulle necessità, e sulle paure, del potenziale elettore possono influenzare il voto di quest'ultimo.

Nell'epoca attuale, le minacce all'autonomia decisionale e alla privacy personale giungono frequentemente attraverso lo spazio cibernetico e da soggetti non immediatamente identificabili. Il potenziale cliente e/o l'elettore indeciso non hanno immediata contezza del meccanismo attraverso il quale quello specifico spot della sua bibita preferita o quel determinato messaggio elettorale sono giunti nella sua cartella di posta elettronica o lampeggiano ammiccanti nella schermata del suo profilo *social*. Le persone sono spesso ignare di come i loro dati sono raccolti e utilizzati per scopi commerciali o politici.

Non si vuole qui proporre soluzioni manichee e inattuabili come il rifiuto delle nuove tecnologie digitali per preservare l'autonomia personale, ma una riflessione sul diritto alla privacy e sulla sua evoluzione. Attraverso un simile studio è infatti possibile capirne il vero contenuto e predisporre quindi le adeguate tutele giuridiche nel moderno contesto digitale. Il suddetto diritto trova il suo fondamento nel riconoscimento della privacy come un valore suscettibile di salvaguardia da parte dell'ordinamento normativo[366]. La nozione di privacy non è uniforme e immutabile, ma ha invece subito una costante evoluzione nel corso del tempo, causata anche dalle diverse e mutevoli esigenze della collettività e dai differenti contesti culturali e geografici[367]. Vi sono però delle caratteristiche comuni attraverso le quali è possibile riconoscere nella tutela della privacy la salvaguardia del livello più profondo della vita privata e personale di un individuo, a cui può accedere solo quest'ultimo. Il potere pubblico non è legittimato ad alcuna ingerenza in tale ambito, se non preventivamente autorizzato dalla normativa vigente. Il valore della privacy non è infatti assoluto, ma deve essere contemperato con altri principi altrettanto meritevoli di riconoscimento, come la libertà di informazione e di espressione. Il punto di equilibrio tra queste tensioni contrapposte è cambiato nel corso dei secoli, rispecchiando le diverse esigenze della società e i mutamenti socio-economici che sono intervenuti a influenzare questa relazione. Per poter risolvere questa contrapposizione nel contesto digitale, occorre ripercorrere brevemente l'evoluzione

[366] B.PERINAN, *ibidem.*
[367] S.NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, pp.11 ss.

dell'idea di privacy al fine di valutare quali sono stati gli accadimenti e le riflessioni che sono alla base della situazione attuale.

1.1. Una breve storia dell'idea di privacy: dalla vergogna biblica all'autonomia informativa

Il bisogno di una sfera intima e personale, lontana dalle pressioni pubbliche, è presente nell'essere umano sin dalla notte dei tempi; la violazione di questo spazio privato da parte di soggetti esterni può essere causa di vergogna per l'individuo[368]. La violazione abusiva e indesiderata del proprio spazio può infatti provocare una sensazione di disagio e inadeguatezza. Un chiaro esempio di ciò viene dal testo della Bibbia; non appena Adamo ed Eva si rendono conto di essere nudi, coprono il proprio corpo con foglie di fico[369]. I due progenitori mostrano un'istintiva consapevolezza della violazione della propria privacy e si vergognano delle conseguenze di tale ingerenza[370].

Il concetto di riservatezza cambia durante l'epoca dell'Antica Grecia, assumendo connotati più prettamente sociali e politici; i pensatori e filosofi ellenici tracciano una netta distinzione tra "interno" ed "esterno", tra vita pubblica e privata[371]. Aristotele definisce l'uomo come "animale politico", cioè come individualità che trova la propria ragion d'essere nel prendere parte a un gruppo sociale[372]; la struttura della *polis* greca, dove ogni cittadino svolge una funzione importante per il corretto funzionamento dell'intera collettività, richiede l'attiva partecipazione di ogni persona a ogni fase della vita di comunità. La volontà di ritirarsi dall'*agorà* pubblica viene quindi vista con disapprovazione; il voler trascorrere una vita fuori dalla dimensione sociale è considerato come una scusa per non adempiere ai propri doveri pubblici[373]. I cittadini maschi hanno il preciso dovere civico di contribuire alla sfera politica della propria comunità[374]; chi non adempie a tale compito è considerato come un estraneo dal gruppo sociale di

[368] M.R.KRONVITZ, *Privacy and the law: a philosophical prelude*, in *Law and Contemporary Problems*, n.31, 1966, pp.272-281.
[369] Gen.,3.7, *Allora si apersero gli occhi ad ambedue, e s'accorsero ch'erano ignudi; e cucirono delle foglie di fico, e se ne fecero delle cinture*, https://www.wordproject.org/ (consultato il 5 luglio 2019).
[370] R.F.HICKSON, *Privacy in a public society. Human rights in conflict*, Oxford, 1987, pp.10 ss.
[371] B.MOORE JR, *Studies in social and cultural history*, Armonk NY, 1984, pp.53 ss.
[372] ARISTOTELE , *Politica e Costituzione di Atene*, edizione italiana a cura di C.A.VIANO, Torino, 1955, pp.12 ss.
[373] S.NIGER, *op.cit.*
[374] F.FABRIS, *Il diritto alla privacy tra passato, presente e futuro*, in *Rivista di Scienze della Comunicazione*, n.2, 2009, https://www.openstarts.units.it/bitstream/10077/3394/1/09_fabris.pdf (consultato il 5 luglio 2019).

appartenenza[375]. La necessità di avere una propria dimensione privata è limitata all'espletamento dei propri bisogni primari. Brevi periodi di ritiro sono tollerati, senza venire però meno alle esigenze della collettività; deve essere rispettato l'equilibrio tra il desiderio di una vita privata e la necessità di dipendere dagli altri membri della *polis*[376]. La tutela che le leggi dell'Antica Grecia garantiscono ai confini della proprietà non è infatti a salvaguardia della proprietà privata in quanto tale, concetto ancora estraneo alla mentalità ellenica del tempo, ma è giustificata dal fatto che un uomo senza la propria casa non può partecipare alla vita della città, non avendo in essa un luogo che definisce come proprio[377]. Occorre comunque specificare che il rispetto degli spazi privati erano comunque valori importanti per gli antichi greci; in ambiente domestico, il padre delle divinità veniva venerato come *Zeus Herkeios*, protettore della casa e difensore della dimora dai nemici esterni[378].

Nell'epoca dell'Antica Roma, il concetto di privacy non è esplicitamente riconosciuto e definito normativamente, ma non manca tuttavia una tutela giuridica per le azioni contro la persona e la sua identità individuale[379]. L'*actio iniuriarum* protegge infatti sia il *corpus* che l'*animus*, ossia punisce le aggressioni fisiche e le offese ad aspetti riguardanti la personalità[380]. Può essere esercitata solamente da un cittadino romano, ossia solamente da colui che la *civitas* ritiene meritevole di tutela: è la comunità sociale che dà valore all'identità personale dell'individuo. L'azione in esame si applica ai casi di diffamazione e a ogni tipo di offesa che può ledere l'onore e la reputazione del cittadino[381]. A differenza di quanto succede nel mondo ellenico, la cultura romana inizia a prestare attenzione alla sfera individuale, andando a sanzionare i comportamenti che procurano una lesione all'intimità e al buon nome del *cives* romano. La diffusione del cristianesimo contribuisce grandemente alla valutazione della dimensione privata dell'individuo. La morale cristiana pone l'accento sul rispetto della persona e sulla sacralità della famiglia; il fedele non deve giudicare il prossimo interferendo nella sua vita personale, poiché conta solo il giudizio divino.

---

375 "*Un uomo che vivesse solo una vita privata e che, come lo schiavo, non potesse accedere alla sfera pubblica o che, come il barbaro, avesse scelto di non istituire un tale dominio, non era pienamente umano*" da H.ARENDT, *Vita activa. La condizione umana*, Milano, 2001, pp.19.

376 J.HOLVAST , *History of privacy*, in (a cura di)K.DE LEEUW, J.BERGSTRA, *The History of Information Security: a Comprensive Handbook*, 2007, Amsterdam, pp.739 ss.

377 S.NIGER, *op.cit.*

378 J.D.MIKALSON, *Ancient Greek religion*, Londra, 2009, pp.23 ss.

379 B.PERINAN, *op.cit.*

380 R.ZIMMERMANN, *The law of obligations. Roman foundations of the civilian tradition*, Oxford, 1996, pp. 1052.

381 D.J.IBBETSON, *A historical introduction to the law of obligations*, Oxford, 1999, pp.112 ss.

L'idea di privacy subisce un'ulteriore evoluzione in epoca medievale. Il crollo dell'Impero Romano lascia un enorme vuoto di potere; la *res publica* è collassata e con essa l'allora tradizionale rapporto tra la persona e la dimensione pubblica. Gli individui si rifugiano all'interno di castelli e roccaforti, formando nuovi modelli di vita e schemi relazionali. Durante tali anni, il termine privato assume quindi il significato di familiare[382]. Il buon funzionamento della società medievale è dato dalla fiducia che unisce i membri della collettività, non dando spazio ad alcuna individualità. Ne è un chiaro esempio la *commendatio*: con tale termine si indica l'atto con cui una persona si affida *in toto* al capo della corte nobiliare, creando un solido legame, indistruttibile per qualsiasi potere pubblico esterno, con lui e con gli altri membri del gruppo[383]. L'avvento del sistema feudale ha portato a una sostanziale parcellizzazione del potere pubblico; ogni singolo castello agisce come "Stato" a sé stante, in una fitta rete di relazioni e scambi commerciali con le altre dimore signorili. Questa nuova situazione politica permette a ogni persona di avere una propria dimensione privata, protetta dall'intimità della propria corte feudale. In questa epoca si inizia quindi ad avvertire il desiderio di intimità e la volontà di guadagnare l'autonomia della propria sfera emotiva e intellettuale; è il primo passo che porta le persone a voler essere considerate individualmente andando a rompere la divisione tra feudatari e popolo tipica dell'epoca[384].

La colonizzazione delle Americhe è un ulteriore elemento che contribuisce all'evoluzione del moderno concetto di privacy; la distanza tra le proprietà terriere nelle vaste lande inesplorate del nuovo continente permette a ogni persona di poter avere la propria intimità[385]. La casa si afferma come dimensione riservata e privata, in cui può accedere solamente chi ha il permesso del proprietario. La privacy si collega perciò all'idea di ricchezza e benessere economico; solamente chi ha le disponibilità per poter comprare un proprio spazio può permettersi la propria intimità, mentre tale possibilità rimane preclusa al povero e all'indigente.

L'evoluzione del diritto alla riservatezza si intreccia indissolubilmente con l'idea di proprietà privata: nel 1890 la privacy viene definita come *right to be let alone*,

---

[382] F.FABRIS, *op.cit.*

[383] La *commendatio* era la cerimonia con la quale, durate l'Alto Medioevo, il signore sceglieva il suo vassallo. Per un'analisi completa di tale rito e delle conseguenze sociali e giuridiche che ne derivavano, si veda G.DUBY, *Potere privato, potere pubblico,* in (a cura di) P.ARIES,G.DUBY, *La vita privata,* Vol.II, Roma-Bari, 2001, pp.10 e ss.

[384] L.MUMFORD , *La cultura delle città,* Milano, 1967, pp.53 ss.

[385] D.FLAHERTY, *Privacy in colonial New England,* Charlottensville, 1972, pp.7 ss.

letteralmente il diritto a essere lasciati soli[386] e a non subire ingerenze esterne. Tale diritto si afferma come prerogativa della classe borghese, che sente la necessità di appropriarsi del proprio spazio riservandosi la prerogativa di decidere in maniera autonoma con chi condividerlo; l'influenza dello schema del diritto alla proprietà privata risulta evidente[387]. Viene riconosciuta alla persona la possibilità di veder salvaguardata la propria potestà su aspetti non strettamente fisici e concreti, come i pensieri formulati o le parole espresse. Il *right to be alone* diventa un diritto negativo che assicura la protezione contro l'indebito disvelamento di fatti privati[388] da parte di terzi; si avverte la necessità di trovare un punto di equilibrio tra il diritto alla riservatezza e la libertà di informazione. Ci si interroga non sulle modalità attraverso le quali una notizia relativa a una specifica persona deve essere divulgata, ma sull'effettiva opportunità di diffondere tale informazione[389].

Il tema della libertà di espressione e della circolazione delle notizie non è certamente una novità del XXIX secolo: la legge[390] sulla libertà della stampa francese del 1881 proibisce la pubblicazione di fatti relativi a un individuo senza che questi abbia dato il suo preventivo assenso o se gli accadimenti non sono ancora di dominio pubblico. Il diritto alla libertà di stampa è riconosciuto da importanti documenti dell'epoca o addirittura risalenti, come la Costituzione federale degli Stati Uniti (1787) o il *Bill of Rights* britannico (1689).

Il bilanciamento tra privacy e stampa si impone al centro del dibattito giuridico e politico dell'epoca per le importanti novità tecnologiche che permettono al mercato dell'informazione di compiere un rilevante salto di qualità. Robert Barclay inventa nel 1875 la cd.stampa in *offset*, utilizzata poi dai maggiori giornali per garantire una maggiore tiratura; nel 1837 Louis Daguerre sviluppa la prima fotografia. Il 1851 vede la nascita di uno dei quotidiani più famosi di ogni epoca, il *The New York Times*. Gli strumenti forniti dal progresso tecnologico consentono ai giornali di fine Ottocento di aumentare le proprie tirature e diffondere maggiormente le notizie pubblicate, ma anche di infrangere la privacy delle singole persone in maniera molto più facile ed economica.

---

[386] S.D.WARREN, L.D.BRANDEIS, *The right to privacy*, in *Harvard Law Review*, vol.4, n.5, 1890, pp.193-220.
[387] M.GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Espaço Juridico Journal of Law*, vol.14, n.1, 2013, pp.149-190.
[388] W.PROSSER, *Privacy*, in *California Law Review*, vol.48, n.3, 1960, pp.384.
[389] G.TROIANO, *Privacy, che ci insegna la Storia sulle differenze tra Usa ed Europa*, in *Agenda Digitale*, https://www.agendadigitale.eu/sicurezza/breve-storia-della-privacy-ue-e-usa-a-confronto/ (consultato l'8 luglio 2019).
[390] *Loi du 29 juillet 1881 sur la liberté de la presse*, w.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722 (consultato l'8 luglio 2019).

Matura una consapevolezza in materia di dati personali e la necessità di mantenere una signoria su di essi; gradualmente la prospettiva si sposta da un diritto alla riservatezza a un diritto all'autonomia informativa. La persona deve essere in grado di decidere sulle modalità in cui i propri dati vengono condivisi e per quali finalità. Nell'epoca attuale la connessione informatica globale non permette più "di essere lasciati soli"; chi non è presente nel *cyberspace* rischia di non avere un posto nella collettività.

La necessità avvertita maggiormente nel contesto digitale non è perciò quella di avere una sfera personale e inviolabile, poiché tale circostanza non è più possibile nello spazio cibernetico, ma di avere una piena potestà sui propri dati, affinchè la loro diffusione avvenga sotto il controllo del soggetto a cui si riferiscono non causando alcun danno all'identità personale.

1.2. L'idea di privacy nei diversi contesti sociali e geografici

La diffusione capillare di Internet ha reso il mondo diventasse più piccolo. La tecnologia attualmente disponibile ci permette di comunicare con ogni angolo della Terra a una velocità istantanea e con costi irrisori. Lo spazio cibernetico non conosce confini geografici o politici e annulla le distanze tra gli utenti informatici. Il superamento delle tradizionali barriere giuridiche comporta però dei potenziali rischi per la tutela della privacy di coloro che navigano lo spazio cibernetico; una potenziale lesione della loro autonomia informativa può infatti avere conseguenze non prevedibili in maniera preventiva. I dati degli utenti vengono infatti quotidianamente condivisi in ogni parte del globo e sono processati attraverso *server* spesso localizzati a migliaia di chilometri dal luogo di connessione.

La problematica della privacy digitale deve essere quindi affrontata in una prospettiva globale; non è possibile identificare una soluzione a livello dei singoli ordinamenti nazionali. Non bisogna però dimenticare che il concetto di privacy è il frutto di una lunga elaborazione giuridica e politica, motivata dalle necessità della collettività sociale. Le esigenze della società sono però soggette a continui cambiamenti e mutazioni, anche a causa dei diversi contesti culturali ed economici. Non esiste un unico concetto di privacy, immutabile al cambiamento dei diversi fattori, poiché ogni cultura ha sviluppato una diversa idea di riservatezza e autonomia informativa, realizzando anche appositi strumenti e metodi per tutelare tali valori.

Per comprendere appieno le rispettive esigenze di ogni gruppo sociale e per valutare se l'attuale normativa europea e internazionale può proteggere adeguatamente il diritto all'autonomia informativa su una scala globale, occorre perciò partire da una preventiva analisi del concetto di privacy nei diversi contesti geografici.

1.2.1. L'idea di privacy nella cultura africana: dal pensiero collettivo della filosofia Ubuntu all'individualismo moderno

Come si evince dalla sua evoluzione storica, la tutela della privacy nella cultura europea e americana è volta alla salvaguardia dell'individuo e delle sue prerogative[391]. La normativa in materia pone al centro dell'attenzione la persona in quanto tale, salvaguardandone l'individualità, l'autonomia e la possibilità di stringere in maniera indipendente relazioni interpersonali[392] e permettendole di raggiungere i propri obbiettivi in termini di autorealizzazione[393]. Questa prospettiva comporta una possibile tensione tra il diritto alla privacy, ritenuto una prerogativa individuale, e le necessità della collettività nel suo insieme[394]; per questa ragione, l'attenzione alla riservatezza e alla salvaguardia della propria sfera personale può essere vista come controproducente rispetto ai bisogni della società[395].

Un'analisi dell'elaborazione culturale dell'idea di privacy nel contesto dell'America Latina porta a simili conclusioni, seppur con la necessità di fare alcune significative distinzioni. La cultura sudamericana sottolinea l'importanza del dato personale e dell'autonomia informativa, sviluppando il concetto di *habeas data*[396], ossia il diritto di avere la potestà sui propri dati, sulla scia del diritto all'*habeas corpus* di elaborazione britannica.

La situazione del continente africano presenta invece delle peculiarità che la contraddistinguono dalla riflessione in materia di privacy maturata nella cd. cultura occidentale e che meritano una breve analisi.

---

[391] L.A.BYGRAVE, *Privacy in a global context – A comparative overview*, in *Scandinavian Studies in Law*, vol.47, 2004, pp.319-348.
[392] L.A.BYGRAVE, *Data protection law: approaching its rationale, logic and limits*, Londra, 2002, pp.138-143.
[393] A.F.WESTIN , *Privacy and freedom*, New York, 1970, pp.39 ss.
[394] P.M.REGAN, *Legislating privacy: technology, social values and public policy,* pp.32 ss.
[395] R.A.POSNER, *The right to privacy*, in *Georgia Law Review*, vol.12, 1978, pp.393-422.
[396] A.GUADAMUNZ, *Habeas data: the Latin American response to data protection*, in *Journal of Information Law and Technology*, n.1, 2000, https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz/ (consultato il 9 luglio 2019).

La visione tradizionale vede infatti l'Africa come un luogo dove la singola individualità non ha spazio per emergere e per raggiungere una propria autodeterminazione, poiché la società è fondata su una base prettamente famigliare[397] dove i membri sono legati tra di loro da vincoli di interdipendenza; il clan, la famiglia o la tribù hanno un valore gerarchicamente superiore rispetto all'individuo di per sé[398] e danno un significato alla vita del singolo uomo. Il pensiero filosofico *Ubuntu*[399] considera disdicevole l'autodeterminazione dell'individuo se non viene permessa dall'intera collettività e se va contro i bisogni del gruppo sociale di origine[400]; non è contemplata l'idea di proprietà privata e il lavoro viene condotto in un'ottica collettiva. Le dispute e le controversie vengono risolte all'interno del gruppo famigliare per promuoverne la coesione.

La prospettiva di *Ubuntu* è però da considerarsi maggiormente come un retaggio della tradizione africana piuttosto che un elemento caratterizzante la realtà odierna[401]. Le nuove tecnologie di coltivazione permettono colture individuali senza il bisogno di ricorrere all'aiuto della famiglia, incentivando anche l'acquisto di singoli appezzamenti di terra. Le reti digitali e i nuovi mezzi di comunicazione hanno inoltre contribuito a introdurre nel continente africano modelli culturali di ispirazione occidentale, basati sull'individualismo e sulla realizzazione personale. I valori di *Ubuntu* sono quindi ancora presenti nel contesto sociale africano, ma non sono più dominanti.

L'idea di privacy non fa eccezione e la riflessione africana in tale tema risente dell'influenza europea e anglosassone: tale concetto coincide con la condizione individuale caratterizzata dall'esclusione dalla vita sociale. Rientrano in tale situazione anche i fatti personali che il soggetto vuole tenere esclusivamente privati, non conoscibili dall'opinione pubblica[402].

L'elaborazione giuridica in materia di diritto alla privacy nel continente africano è però relativamente recente, frenata dagli elementi culturali a cui si faceva prima

---

[397] E.J.LASSITER, *African culture and personality: bad social science, effective social activism or a call to reinvent ethnology?* in *African Studies Quarterly*, vol.3, 2000, pp.1-21.
[398] A.B.MAKULILO , *"A person is a person through other persons" – A critical analysis of privacy and culture in Africa*, in *Beijing Law Review*, n.7, 2016, pp.192-204.
[399] Per un'introduzione al pensiero filosofico *Ubuntu,* si veda; R.BOLDEN, *Ubuntu*, in (a cura di)D.COGHLAN, M.BRYDON-MILLER, *Encyclopedia of Action Research*, Londra, 2014, pp.39-78.
[400] M.N.KAMWANGAMALU, *Ubuntu in South Africa: a sociolinguistic perspective to a Pan-African concept*, in *Critical Arts: South-North Cultural Media Studies*, n.13, pp.24-41.
[401] A.B.MAKULILO , *op.cit.*
[402] J.NEETHLING, *The concept of privacy in South African law*, in *The South African Law Journal*, vol.122, n.1, 2005, pp. 18-28.

riferimento. La Carta Africana sui Diritti dell'Uomo e dei Popoli[403], stipulata nell'ambito dell'organizzazione regionale *Organization of African Unity*, il 27 giugno 1981, è l'unico strumento internazionale formulato nel XX secolo in materia di diritti fondamentali a non elencare al suo interno anche il diritto alla privacy.

La tradizionale suddivisione della struttura sociale africana in singoli gruppi, come i clan, le famiglie o le tribù, si pone infatti in netto contrasto con la controparte occidentale basta invece sulla singola persona e sull'individualismo che sono condizioni che favoriscono la richiesta di riservatezza e autonomia. La priorità accordata agli interessi della collettività rispetto a quelli della persona in quanto tale rappresenta un indubbio ostacolo alla formazione di una normativa unitaria e stabile in materia di diritto alla privacy[404].

Non bisogna però cadere in un acritico parallelismo in cui la società occidentale, caratterizzata da una forte impronta individualistica, e la società africana definita dal pensiero collettivista di *Ubuntu* si fronteggiano come mondi opposti. La crescente urbanizzazione ha i contribuito a creare nuovi centri cittadini rompendo i modelli di coesione sociale tipici della tradizione culturale africana[405]. La modernizzazione delle metodologie di coltivazione della terra ha inoltre rivoluzionato l'agricoltura del continente, dove le fattorie a gestione famigliare non sono più la norma. Le reti digitali e i mezzi di comunicazione hanno poi introdotto nella società africana lo stile di vita occidentale e i concetti di individualismo e realizzazione personale che sono alla base della moderna concezione di privacy. La diffusione di Internet e delle problematiche relative all'autonomia informativa sta certamente portando i legislatori africani a formulare normative adeguate in tale materia.

Non bisogna quindi considerare la realtà del continente africano come statica e immutabile, bensì in continuo divenire, sia sotto l'aspetto socio-economico che giuridico. Il retaggio culturale del continente si basa su valori come il collettivismo, la coesione sociale e la predominanza dei bisogni del gruppo su quelli del singolo, ma non bisogna dimenticare che l'Africa non è una realtà a sé stante, ma è pienamente connessa con il resto del mondo e sottoposta alle influenze delle altre culture, anche in tema di diritto alla

---

[403] Organization of African Unity (OAU), *African Charter on Human and Peoples' Rights ("Banjul Charter")*, 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), https://www.refworld.org/docid/3ae6b3630.html (consultato il 9 luglio 2019).

[404] L.A.BYGRAVE, *Privacy in a global context, op.cit.*

[405] M.F.SILHONGONYANE , *The invisible hand of the family in the underdevelopment of Africa societies: an African perspective*, in *Scholarly Paper Series*, n.1, http://www.gdrc.org/icm/country/scholarly/fanafrica.html (consultato il 10 luglio 2019).

privacy. Alla luce di ciò, si può concludere che l'esigenza di una normativa in materia di autonomia informativa è avvertita anche in Africa, pur nel rispetto delle peculiarità e delle necessità della società di quel continente.

2. Una definizione giuridico-filosofica di privacy nel contesto cibernetico: il diritto all'habeas data

L'analisi fin qui condotta permette di formulare alcune prime osservazioni; il concetto di privacy è ben lontano dal potersi definire statico e immutabile, poiché è frutto dell'elaborazione culturale delle diverse epoche. La collettività definisce tale idea secondo gli strumenti del suo tempo e alla luce delle necessità e delle esigenze avvertite; si comprende bene che il diritto alla riservatezza formulato da Warren e Brandeis nel 1890 presenta caratteristiche ben diverse rispetto al diritto all'autonomia informativa di epoca digitale.

Alla luce di ciò, è possibile formulare una definizione giuridica del concetto di privacy che resista al continuo progresso tecnologico e che non costringa il legislatore ad aggiornare frequentemente la normativa vigente?

Numerosi studiosi e accademici hanno cercato di rispondere a questa domanda, concludendo però che l'idea di privacy è un concetto troppo complesso per essere ridotto a una singola essenza; racchiude in sé stesso una pluralità di situazioni e realtà che apparentemente non hanno alcunché in comune, ma che tuttavia mostrano una somiglianza reciproca[406]. Provare a fornire una definizione di privacy senza tenere in considerazione le criticità e le sfide a cui viene sottoposto tale concetto nella società contemporanea può avere un effetto controproducente, limitandone progressi giuridici ulteriori[407].

Il presente studio si basa perciò su tale consapevolezza; l'obbiettivo non è quello di delineare un'idea astratta di privacy, immutabile e valevole a prescindere del progresso tecnologico, ma di calare quest'ultima nel contesto cibernetico per valutarne le peculiarità in tale ambito e ipotizzarne una possibile evoluzione. Solo dopo aver raggiunto questo

[406] D.J.SOLOVE, *Nothing to hide: the false tradeoff between privacyand security,* New Haven CT, 2011, pp.24.
[407] H.F.NISSENBAUM, *Privacy in context:technology, policy and the integrity of social life*, Stanford CA, 2010, pp.2 e ss.

scopo sarà infatti possibile riflettere sulla normativa vigente in materia per esaminarne i lati positivi e i possibili aspetti deficitari.

Nel suo significato fondamentale, la parola "privacy" rimanda agli aspetti più intimi della vita umana, come la famiglia, la casa e la corrispondenza privata[408]. Nel XXIX secolo l'attenzione inizia a spostarsi anche sul controllo delle proprie informazioni, come testimoniato dal già citato scritto di Warren e Brandeis. Il *right to be left alone* formulato dai due studiosi statunitensi si concretizza anche nell'assoluta potestà esercitata dalla persona sulle proprie informazioni: poter decidere quali pensieri, parole e fatti condividere con il resto dell'opinione pubblica. Pur risultando ammirevole per la sua semplicità, il "diritto a essere lasciati soli" non riesce a racchiudere appieno le numerose sfaccettature del concetto di privacy[409].

La rapida evoluzione delle tecnologie di comunicazione avvenuta nel XX secolo ha infatti sollevato nuove problematiche che non potevano esser risolte limitandosi ad applicare il *right to be left alone*, pur rimanendo questo la base da cui partire per un ulteriore studio sul tema.

Gli elementi principali della riflessione accademica in materia di privacy, a partire dalla seconda metà del '900, sono stati i concetti di libertà, autodeterminazione e controllo[410]. La definizione data dal Westin nel 1967 ne è un chiaro esempio: lo studioso americano ritrasse la privacy come la richiesta di persone, sia fisiche che giuridiche, di esercitare una completa signoria sulle informazioni che le riguardassero, per decidere in autonomia quale tra queste potessero essere rivelate all'opinione pubblica. Nei termini di partecipazione alla vita sociale, questa significava la possibilità per ogni individuo di ritirarsi a una dimensione privata, in condizioni di anonimato o riservatezza, secondo le condizioni e le metodologie prescelte dallo stesso[411].

La privacy acquista quindi una duplice dimensione: una relazionale e una informativa. Il primo aspetto riguarda i rapporti della persona con gli altri membri della collettività; ad esempio chi può entrare nello spazio domestico o chi ha il permesso di toccare determinate zone del corpo. Il secondo si concentra invece sui diritti dell'individuo nei riguardi della raccolta e della gestione di informazioni e dati personali. Un aspetto comune a entrambe le prospettive è la volontà dell'essere umano di mantenere

[408] J.HOLVAST, *op.cit.*
[409] P.BERNAL, *op.cit.*
[410] A.F.WESTIN, *Privacy and freedom*, Londra, 1967, pp.47-64.
[411] A.F.WESTIN , *ibidem.*

il controllo su ciò che lo circonda, sia questo il proprio corpo o la propria abitazione nel caso della privacy relazionale oppure i dati personali nell'evenienza di quella informativa. Tale forma di controllo è espressione della volontà di autodeterminazione tipica dell'essere umano e caratteristica dell'elaborazione giuridica e dottrinale della seconda metà del XX secolo in materia di riservatezza, come anticipato poc'anzi.

La relazione e le interconnessioni tra le due dimensioni della privacy meritano un'attenta riflessione[412]. Non è infatti semplice individuare il confine che intercorre tra di esse, intendendole come due aspetti separati e distinti: limitare l'accesso alla sfera privata ostacola anche la circolazione di informazioni relative ad essa. Ma quali informazioni devono essere considerate private? C'è un'effettiva differenza tra i dati "privati" e i dati "personali"? Sono quesiti di non facile risposta, anche a causa della pervasività delle reti digitali, La diffusione di Internet ha radicalmente cambiato i tradizionali meccanismi di comunicazione, comportando una loro totale reinvenzione e il loro adattamento alla situazione cibernetica. L'applicazione della privacy nello spazio cibernetico dovrebbe essere considerata sulla base del contesto[413], analizzando non solo chi ha accesso alla singola informazione, ma tenendo conto anche delle modalità di condivisione, delle finalità e delle tempistiche.

Risulta quindi complesso individuare categorie normative per i vari tipi di dati e informazioni che possano resistere nel tempo; tecnologie sempre più avanzate di profilazione, di *data mining* e di profilazione commerciale propongono sempre nuove sfide al legislatore. Un determinato dato che in una prima occasione può apparire irrilevante può diventare di vitale importanza in un secondo momento.

Un esempio può forse giovare alla comprensione della complessità della realtà informatica[414]; l'acquisto da parte di un cliente di un supermercato di una bevanda senza zucchero può apparire a prima vista irrilevante, se non in un'ottica commerciale, ma può essere un segnale del fatto che quel consumatore è diabetico. Individuare quale informazione è suscettibile di una più approfondita salvaguardia si rivela però un compito spesso improbo che, se non compiuto efficacemente, può causare un *vulnus* importante al diritto all'identità di una persona.

Nel contesto cibernetico, la parola privacy non può essere intesa esclusivamente come volontà della persona di essere lasciata sola, poiché Internet permette una sorta di

[412] P.BERNAL, *op.cit.*
[413] H.F.NISSENBAUM , *op.cit.*
[414] P.BERNAL, *op.cit.*

interconnessione globale tra tutti i membri della collettività; la *data protection* non si concretizza quindi nel nascondere le proprie informazioni[415], ma piuttosto nella gestione della loro condivisione. Il diritto alla tutela dei dati personali assume una dimensione positiva e concreta, a differenza del *right to be let alone* formulato da Warren e Brandeis nell'ormai lontano 1890 che si limitava a pretendere che non vi fossero ingerenze di terzi nella sfera privata della persona; ora l'individuo ha il diritto che i propri dati personali siano registrati, gestititi, custoditi, trasmessi a terzi, divulgati in modo corretto e *secundum legem*.

La *ratio* di un tale diritto è di permettere a ogni individuo di controllare la disponibilità delle informazioni che lo riguardano, autodeterminando così la propria realtà e la propria reputazione nei confronti degli altri membri della collettività, arrivando a impedirne la fruizione da parte di soggetti estranei alla propria dimensione privata[416]. Il valore dell'autodeterminazione informativa permette alla persona, e più specificatamente all'utente cibernetico, di navigare liberamente nel *mare magnum* di Internet, mantenendo però sempre la consapevolezza di quali informazioni condivide e per quali finalità[417].

Ogni cittadino deve avere piena potestà sul proprio "corpo elettronico"[418]: nell'epoca digitale le persone si relazionano con gli altri soggetti attraverso la condivisione dei propri dati. L'identità dell'individuo viene affidata alle modalità in cui tali informazioni sono effettivamente gestite, collegate e condivise; il diritto alla tutela dei dati personali permette che sia il soggetto a definire in maniera autonoma la propria immagine[419]. L'avvento dell'epoca digitale ha quindi comportato un importante passaggio evolutivo; dall'*habeas corpus* si arriva all'*habeas data*[420]. Il denominatore comune tra queste due figure è il controllo esercitato dall'essere umano: verso il proprio corpo nel primo caso e nei confronti delle informazioni che riguardano la persona nel secondo.

La differenza tra il diritto alla protezione dei dati personali e il diritto alla privacy inteso come *right to be left alone* risulta evidente: la Corte di giustizia dell'Unione europea ha avuto modo di sottolineare i tratti distintivi di questi due principi[421],

---

[415] D.J.SOLOVE, *op.cit.*
[416] G.P.CIRILLO, *La tutela della privacy nel sistema del nuovo codice dei dati personali*, Padova, 2004, pp.31 ss.
[417] S.RODOTÀ , *Intervista su Privacy e Libertà,* Padova, 2005, pp.23 ss.
[418] S.RODOTÀ, *ibidem.*
[419] S.RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma, 2014, pp.18 ss.
[420] S.RODOTÀ, *ibidem.*
[421] Corte di giustizia dell'Unione europea, causa C-362/14, *Maximilian Schrems c.Data Protection Commissioner*, 6 ottobre 2015.

descrivendo il secondo come il diritto ad avere uno spazio privato immune da ingerenze esterne, mentre il diritto alla *data protection* si estende alla tutela di ogni informazione riferita o riferibile a una persona identificata o identificabile, quale che ne sia il contenuto o l'oggetto e indipendentemente dal suo carattere pubblico o privato.

L'elemento discriminante si rinviene nel bene oggetto di tutela delle due figure giuridiche appena descritte e nella diversa prospettiva adottata: il diritto alla privacy vuole salvaguardare la dimensione intima della persona secondo un punto di vista prettamente individualistico, mentre il diritto alla tutela dei dati personali tutela la correttezza del trattamento delle informazioni che è sì un diritto dell'individuo, ma anche un interesse della collettività[422]. I valori di trasparenza e legittimità sono infatti fondamentali per il mantenimento di un funzionante ordine democratico[423] e possono essere mantenuti solo se ogni persona ha la piena potestà sui propri dati personali evitando perciò di subire ingerenze esterne più o meno dirette, come nel caso dei calcoli predittivi e delle tecniche manipolative, e mantenendo la propria indipendenza intellettuale ed emotiva.

2.1. Le reti digitali e le sfide per l'autonomia personale nello spazio cibernetico

Lo sviluppo delle reti digitali ha avuto enormi implicazioni per la tutela della privacy; il loro funzionamento richiede la raccolta di enormi quantità di dati personali degli utenti, in maniera tale che il confine tra la vita reale propriamente detta e il mondo digitale si sta assottigliando sempre più. Se, come si accennava poc'anzi, la privacy cibernetica si concretizza non nel bloccare il flusso di informazioni condivise nel *web*, ma piuttosto nel gestirlo adeguatamente, si comprende che la navigazione nel *cyberspace* può avere un impatto devastante sull'integrità della sfera privata di ogni persona[424] e sulla sua autonomia decisionale.

L'integrazione sempre crescente del mondo digitale con quello "reale" e la perenne connessione informatica a cui l'essere umano moderno sembra condannato

[422] M.LAMANUZZI, *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal Regolamento (UE) 2016/679 e nuove responsabilità per gli enti,* http://jus.vitaepensiero.it/news-papers-diritto-penale-e-trattamento-dei-dati-personali-codice-della-privacy-novita-introdotte-dal-regolamento-2016-679-ue-e-nuove-responsabilita-per-gli-en-4763.html (consultato il 26 luglio 2019).
[423] S.RODOTÀ, *Tecnologie e diritti,* Bologna, 1995, pp. 31 ss.
[424] P.BERNAL , *op.cit.*

possono però ostacolare l'effettiva realizzazione di un'autonomia personale e decisionale in diverse maniere[425].

Un primo significativo esempio può essere fatto riguardo al funzionamento dei cd. motori di ricerca. L'elenco dei risultati forniti da questi *software* può infatti influenzare il comportamento dell'utente informatico, che sarà più propenso a cliccare sui primi siti suggeriti rispetto a quelli che si trovano in fondo alla lista. Considerato che l'operato dei motori di ricerca non si basa certo sulla casualità, ma sui dati raccolti in maniera tale da fornire all'utente servizi sempre più personalizzati, occorre chiedersi se la persona è effettivamente "libera" di fare le proprie scelte quando naviga nel *cyberspace* o è effettivamente guidata dagli algoritmi informatici.

I meccanismi di profilazione sono una delle possibili minacce più rilevanti all'autonomia decisionale degli utenti cibernetici. Il loro utilizzo in campi come la comunicazione politica apre infatti scenari su cui occorre riflettere: i potenziali elettori possono essere raggiunti attraverso Internet e i *social media* da spot elettorali che puntano a fare leva sui loro pensieri e anche sulle loro paure. A mero titolo di esempio, un utente, identificato attraverso l'analisi dei suoi dati come di idee conservatrici, potrebbe essere influenzato da un messaggio politico incentrato sui "pericoli" insiti nel pensiero liberale. Lo scandalo *Cambridge Analytica*[426] ha mostrato in maniera chiara e inequivocabile cosa può succedere alla privacy e all'autonomia decisionale di ogni singolo individuo quando i dati che lo riguardano non vengono gestiti secondo la normativa vigente, ma vengono invece utilizzati per campagne pubblicitarie di profilazione degli utenti cibernetici, anche in ambito politico-elettorale.

Cambridge Analytica era il nome di nome di una società di consulenza britannica con sede nella capitale Londra, specializzata nell'utilizzo di tecnologie di Intelligenza Artificiale per la raccolta e l'analisi dei dati di utenti Internet e dei principali *social network*. L'esame di queste informazioni permetteva poi di stilare profili altamente specifici delle singole persone; la provenienza geografica, l'età, l'orientamento sessuale, le preferenze politiche, il grado di istruzione erano solo alcuni degli elementi presi in considerazione da *Cambridge Analytica* per prevedere il futuro comportamento delle singole persone e cercare quindi di orientarlo secondo gli obbiettivi della società stessa e

[425] P.BERNAL, *op.cit.*
[426] Per un'analisi approfondita dei fatti relativi a *Cambridge Analytica*, si rimanda all'approfondimento del Guardian: https://www.theguardian.com/news/series/cambridge-analytica-files (consultato il 9 aprile 2020).

dei loro clienti. Si comprende subito quale potenzialità dirompente potesse avere un simile approccio nel campo della comunicazione politica, orientando il voto dei potenziali elettori in un determinato senso piuttosto che un altro. Attualmente sono ancora in corso le indagini per valutare l'effettivo coinvolgimento di *Cambridge Analytica* nelle campagne elettorali per l'elezione di Donald Trump e per il referendum sulla Brexit.

La pratica del *microtargeting* non è certamente una novità introdotta dalla società britannica, dato che viene utilizzata da diverso tempo in molti ambiti commerciali. La raccolta di informazioni sui potenziali consumatori permette infatti alle aziende e alle industrie di produrre degli annunci pubblicitari personalizzati sui gusti e le esigenze della singola persona, cercando quindi di orientarne le future scelte di acquisto. Vengono perciò superate le tradizionali categorie di pensiero che vedevano il pubblico come una massa indifferenziata priva di ogni particolarità individuale, sulla quale il mezzo di comunicazione aveva il medesimo impatto uniforme[427].

L'*audience* non è infatti un'entità meramente passiva, poiché sviluppa un grado di partecipazione diverso a seconda del contenuto trasmesso e del mezzo di comunicazione utilizzato[428]. Questo cambio di paradigma è alla base dell'efficacia del *microtargeting* con scopi commerciali: il potenziale consumatore reagisce in maniera diversa a stimoli differenti. Ogni soggetto ha le proprie peculiarità che vengono stimolate da annunci pubblicitari specifici e personalizzati.

Da un punto di vista prettamente giuridico e di tutela dei diritti fondamentali, in questo caso si ravvisa un potenziale pericolo per la protezione dei dati personali se le informazioni raccolte nelle operazioni di *microtargeting* vengono utilizzate in maniera abusiva e illegittima. Per quanto riguarda il piano della comunicazione politica personalizzata, occorre fare alcune riflessioni preliminari di stampo sociologico-comunicativo.

Il modello dell'*audience* attiva[429] prevede una stretta relazione tra l'individuo, il contesto sociale e il messaggio trasmesso dal mezzo di comunicazione; questo rapporto può concretizzarsi in molteplici esiti che portano ogni soggetto a recepire un particolare significato da quel messaggio. Ogni persona decodifica lo specifico contenuto con

---

[427] W.RUSSELL NEUMAN, *The evolution of media effects theory: a six-stage model of cumulative research*, in *Communication Theory*, n.21 (2), 2011, pp.169-196.
[428] M.DEUZE, *Ethnic media, community media and participatory culture*, in *Journalism*, n.7, 2006, pp.262 ss.
[429] P.F.LAZARSFELD, R.K.MERTON, *Mass communication popular taste and organized social action*, https://scinapse.io/papers/2606081992 (consultato il 9 aprile 2020).

modalità e interpretazioni diverse, a seconda di diverse variabili come la propria posizione sociale o ideologia politica[430]. Questo può non sollevare particolari preoccupazioni quando il cliente deve scegliere la bevanda gassata o il detersivo da comprare, ma occorre riflettere sulle conseguenze che ha un'operazione di *microtargeting* in merito all'autonomia individuale e all'autodeterminazione della persona in campo politico.

Un qualsiasi approccio normativo volto a regolamentare la comunicazione politica attraverso gli strumenti digitali deve tenere ben presenti queste considerazioni.

Il potenziale elettore viene monitorato nel suo comportamento *on-line*; le sue abitudini, le sue attività, le sue preferenze sono tutti elementi che permettono di inviare un messaggio elettorale ben preciso. Una campagna pubblicitaria di *microtargeting* elettorale si basa sugli annunci e le promesse politiche che avranno probabilmente più impatto sull'elettorato, andando a innescare sentimenti di partecipazione tra la cittadinanza. Si arriva al risultato per cui la politica di una nazione viene decisa in base a quale *post* ha ricevuto più *likes* su Facebook.

Il GDPR prevede un divieto esplicito di trattamento per informazioni considerate sensibili e che possono quindi rivelare le opinioni politiche e l'ideologia di una specifica persona (art.9 comma 1). Il Regolamento prevede una deroga a tale disposizione per quanto riguarda i dati resi manifestamente conoscibili dall'interessato (art.9, comma 2, lettera e), ma tale eccezione deve essere interpretata in maniera restrittiva e proporzionale allo scopo legittimo del trattamento.

Le operazioni di *microtargeting* possono avere ricadute positive, come convincere un cittadino a interessarsi della cosa pubblica perché sollecitato da un particolare tema, ma hanno alla base delle tecniche di manipolazione comportamentale da disciplinare con cautela e attenzione. Un partito politico potrebbe decidere di non inviare alcun messaggio a una determinata categoria di persone, escludendole quindi dalla scena pubblica, o di trasmettere contenuti che alterano la percezione della realtà portando quindi i potenziali elettori a modificare il loro comportamento, e di conseguenza le scelte elettorali, su basi erronee. Il diritto alla libera espressione risulta a rischio: il cittadino deve poter usufruire di informazioni attendibili sulle quali formare la propria opinione e successivamente esprimerla. Si assiste invece a un progressivo superamento del concetto di verità fattuale: i fautori di opposti schieramenti politici non sono divisi solamente da ideologie e

[430] B.SAETTA, *Disinformazione e manipolazione. Il pericolo è il microtargeting degli annunci politici*, https://www.valigiablu.it/disinformazione-manipolazione-microtargeting/ (consultato il 9 aprile 2020).

convinzioni differenti, ma fanno riferimento anche a realtà diverse che vengono propugnate come assolute dai rispettivi leader politici.

Si devono evidenziare anche possibili problemi in merito ai profili di privacy e protezione dei dati personali. Il GDPR afferma che ogni trattamento di dati personali deve essere condotto secondo i criteri di liceità, correttezza e trasparenza (art.5). Ponendo l'attenzione sul caso della profilazione, il Regolamento vieta inoltre che l'interessato sia sottoposto a decisioni basate interamente su processi automatizzati a meno che non vi abbia espressamente consentito o perché tale trattamento è autorizzato da altra norma dell'Unione europea (art.22). Quando una pubblicità elettorale diventa invadente o rischia di alterare la percezione del potenziale elettore, questa diventa illegittima ai sensi del GDPR.

2.1.1. Il consenso al trattamento dei dati personali nel contesto cibernetico può dirsi effettivamente libero e informato?

Un'ulteriore tema meritevole di attenzione per quanto riguarda l'integrità dell'autonomia decisionale nel contesto cibernetico è il consenso al trattamento dei dati personali[431].

Come si avrà modo di esaminare nel proseguo dell'analisi, una delle basi di legittimità per la raccolta e la gestione delle informazioni che lo riguardano è la disponibilità del soggetto interessato, che deve acconsentire al loro trattamento in maniera espressa e informata. Le circostanze della navigazione nello spazio cibernetico rendono però complesso valutare se questi requisiti vengono costantemente soddisfatti; solitamente l'utente si limita a cliccare "Ok" senza prestare alcuna attenzione sul lungo modulo informativo che gli viene proposto. Formalmente il consenso è stato effettivamente prestato dopo che il responsabile del trattamento ha fornito le informazioni all'interessato, ma cosa succede effettivamente?

Nel 2010, un'azienda di videogiochi sottopose ai propri utenti un modulo leggermente modificato: era stata infatti inserita una clausola per la quale i clienti si impegnavano a concedere alla compagnia la propria "anima immortale" senza alcun

[431] P.BERNAL, *op.cit.*

corrispettivo in cambio; circa 7.500 utenti acconsentirono a questo scambio[432]. Questo è un chiaro esempio di come la modalità di richiesta del consenso denominata *click wrap* rappresenta un serio pericolo per la privacy e l'autonomia degli utenti cibernetici, che spesso non hanno gli strumenti necessari per leggere e comprendere effettivamente le modalità di raccolta a cui i loro dati sono sottoposti.

Frequentemente gli ISP (*Internet Service Providers*) cercano di ampliare l'utilizzo di tali moduli; avvertono infatti che la raccolta dei dati dei clienti non si limita a quelli generati dal servizio nel cui ambito il consenso è effettivamente prestato, ma anche agli altri prodotti forniti dalla stessa compagnia. Un utente iscritto al servizio di posta elettronica *Gmail* sarà sottoposto al trattamento dati anche durante l'utilizzo di altri servizi *Google,* come *Google Search* o *Google Maps,* senza esserne effettivamente informato. Risulta quantomeno dubbio che in casi del genere la prestazione del consenso possa definirsi legittimamente acquisita.

La questione principale a cui deve rispondere un'analisi giuridica in merito al consenso informatico nel contesto cibernetico non è tanto sulle modalità attraverso le quali questo possa dirsi legittimo e legale, ma piuttosto come renderlo più simile possibile al consenso prestato nel mondo "reale"[433]. Considerate infatti le numerose e ormai ineludibili interconnessioni tra la dimensione fisica e quella digitale, la persona dovrebbe avere le stesse possibilità e capacità in entrambi gli ambiti; la normativa dovrebbe perciò intervenire per rendere possibile un consenso "reale" nel mondo "virtuale".

Si auspica che l'utente possa prendere una decisione effettivamente ponderata e questo è possibile solo dopo la piena comprensione delle informazioni ricevute dal responsabile del trattamento.

A tal proposito, è stato coniato il concetto di "autonomia collaborativa[434]" per descrivere un nuovo approccio al tema del consenso informato in campo medico-sanitario, ma applicabile anche al contesto cibernetico. Secondo questa teoria, il paziente deve essere accompagnato attraverso un continuo dialogo con i medici e la struttura sanitaria a recepire ogni notizia necessaria per avere un pieno ed effettivo consenso informato.

---

[432] *7.500 online shoppers unkowingly sold their souls*, *https*://www.foxnews.com/tech/7500-online-shoppers-unknowingly-sold-their-souls (consultato l'11 luglio 2019).
[433] P.BERNAL, *op.cit.*
[434] H.TEFF, *Reasonable care: legal perspectives on the Doctor-Patient relationship*, Oxford, 1994, pp.198 ss.

Pur tenendo presente le differenze tra il mondo della medicina e quello dell'informatica e delle reti digitali, un simile approccio può forse funzionare anche nello spazio cibernetico. Il consenso dell'interessato non dovrebbe perciò limitarsi alla semplice e istantanea firma di un modulo precompilato, ma si concretizzerebbe in una relazione continua e duratura con il responsabile del trattamento.

Le enormi potenzialità comunicative della rete Internet renderebbero possibile un tale risultato: l'ISP che intrattiene un continuo dialogo con l'utente cibernetico al fine di permettere a quest'ultimo di comprendere appieno tutte le sfaccettature della raccolta e della gestione a cui i suoi dati sono sottoposti. Il processo rispetterebbe i più rigorosi standard di trasparenza permettendo di controllare l'effettivo operato delle grandi compagnie informatiche.

3. La privacy come diritto fondamentale nel contesto cibernetico

L'analisi condotta fin ora ha permesso di enucleare alcune caratteristiche fondamentali della privacy. Essendo frutto di una costante elaborazione socio-culturale, tale principio si è evoluto nel corso degli anni per rispondere in maniera efficace alle mutate esigenze e necessità della collettività. La natura stessa di tale principio, multiforme e sfaccettata, ha portato a un costante mutamento della normativa in materia, privilegiando di volta in volta determinati aspetti a scapito di altri.

Considerato ciò, occorre chiedersi se esiste un vero e proprio diritto alla privacy e se tale principio possa essere giuridicamente definito in maniera tale che non occorra aggiornare la normativa corrispondente a ogni innovazione tecnologica. Lo scopo della riflessione è quindi quello di individuare delle caratteristiche immutabili di suddetto diritto e che non possono essere influenzate dal progresso informatico e digitale.

Come si è visto, la privacy è un elemento imprescindibile per garantire un'autonomia personale sia intellettuale che emotiva; senza un'adeguata protezione della sfera intima, una persona non può ritenersi libera di esprimere la propria opinione e di agire nel contesto sociale senza temere ripercussioni. Il diritto alla privacy deve perciò ritenersi dotato di un carattere fondamentale e assoluto di per sé o riveste piuttosto una

funzione strumentale volta a permettere l'applicazione di altri diritti universalmente riconosciuti, come quello alla libertà di pensiero?

La risposta a queste domande può incidere sulle metodologie di tutela utilizzate per il diritto alla privacy: se si considera quest'ultimo come fondamentale, la normativa deve permettere un'azione diretta del soggetto interessato dalla lesione. In caso contrario, si deve valutare se tale abuso ha influito sulla corretta applicazione del diritto primario, ad esempio quello alla libera espressione.

Una simile riflessione deve necessariamente prendere le mosse dall'evoluzione del concetto di privacy nel contesto cibernetico, inquadrabile ora come diritto all'autonomia informativa, ossia avere consapevolezza di quali informazioni personali si stanno condividendo e per quali finalità.

3.1. Il diritto all'autonomia informativa come prerogativa della persona

Il punto di partenza da cui iniziare un (auspicabilmente) proficuo esame del diritto alla privacy è il concetto di dato. Lo sviluppo dei calcolatori informatici ha permesso la creazione di macchine che producono costantemente un'enorme quantità di informazioni, misurabili nell'unità chiamata *bit*[435] e concretizzata nell'espressione binaria di 0 e 1. Lo sviluppo di Internet ha reso possibile collegare tali macchine in una rete di ricerca, trasmissione e condivisione dei dati; in un primo momento erano inclusi solo i terminali "fissi", ma ora ne fanno parte anche i *device* portatili. La connessione ha quindi raggiunto un grado di pervasività e ubiquità che può solo crescere con il passare del tempo; è un fenomeno in naturale espansione, poiché i dati non archiviati producono altri dati[436].

Il dato è perciò diventato un elemento fondamentale e caratteristico della società digitale; può funzionare sia come "moneta", considerato l'enorme valore commerciale che riveste per aziende e imprese, che come modalità di identificazione della persona a cui si riferisce. Si stanno affermando due diversi concetti di identità, sia fisica che digitale; con quest'ultima si vuole intendere la mole di dati presenti nello spazio cibernetico che contribuiscono a descrivere una persona e le sue azioni.

---

[435] Per una completa spiegazione delle unità di misura in campo digitale e informatico, si rimanda a https://web.stanford.edu/class/cs101/bits-bytes.html (consultato il 15 luglio 2019).

[436] V.ZENO-ZENCOVICH, *Il concetto di "autonomia privata" ai tempi dei "Big Data"*, in (a cura di) P.PASSAGLIA, D.POLETTI, *Nodi virtuali, legami informali: Internet alla ricerca delle regole*, Pisa, 2017, pp.31-37.

I sistemi tradizionali di tutela dell'identità personale non sono in grado offrire le adeguate garanzie giuridiche nel contesto digitale, poiché le minacce che devono affrontare non erano minimamente preventivabili al momento della loro ideazione; occorrono perciò nuovi strumenti atti a tale funzione.

Gli utenti cibernetici condividono quotidianamente un'enorme quantità di informazioni personali navigando nel *web* e questa condivisione può avvenire più o meno consapevolmente[437]. Ad esempio, possono acconsentirvi al momento della stipulazione di un contratto con un ISP per fruire di determinati servizi informatici, ma d'altra parte anche le stesse reti digitali necessitano di acquisire e processare i dati dei propri utenti per funzionare.

La grande varietà di informazioni[438] presenti nel *cyberspace* e la disponibilità di tecnologie sempre più sofisticate utilizzabili per raccogliere e processarle comporta la presenza di rischi sempre maggiori per la privacy delle persone[439]. Una simile realtà dei fatti comporta delle specifiche conseguenze; *in primis* la necessità di un'adeguata tutela normativa per evitare che la privacy e la sfera privata di qualsiasi individuo possa subire attacchi e ingerenze da parte di terzi e per assicurare a ogni persona la possibilità di esercitare una completa potestà sulle informazioni che la riguardano.

Il diritto alla privacy si afferma quindi nel contesto digitale come strettamente connesso ai valori di libertà e individualità e come condizione imprescindibile per l'individuo per compiere le più disparate scelte all'interno del contesto sociale, come iscriversi a un partito politico, professare una determinata fede religiosa o seguire uno specifico orientamento sessuale[440]. L'obbiettivo a cui deve tendere il legislatore non è, o perlomeno non solo, quello di garantire l'adeguata sfera di riservatezza alla persona, ma di proteggere i suoi dati personali: da diritto alla privacy si passa al diritto alla *data protection* e all'autonomia informativa.

L'opinione maggioritaria[441] annovera tale principio nei diritti della personalità per diverse ragioni. Vengono ravvisate somiglianze nelle finalità, consistenti nella

---

[437] M. GAMBINI, *op.cit.*

[438] R.D'ORAZIO, *Dati personali in rete aperta,* in (a cura di) V.CUFFARO, V.RICCIUTO, *Il trattamento dei dati personali. Profili applicativi*, Torino, 1999, pp.276-373.

[439] S.RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, pp.10 ss; V.FROSINI, *Il diritto nella società tecnologica*, Milano, 1981, pp.15 ss.; M.GAMBINI, *op.cit.*

[440] M.GAMBINI, *op.cit.*

[441] Si veda, a mero titolo di esempio, G.MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Diritto dell'Informatica,* 1997, pp.317 ss.; G.ALPA, *La normativa sui dati personali: modelli di lettura e criteri esegetici*, in *Diritto dell'Informatica*, 1997, pp.703 ss.; V.ZENO-ZENCOVICH, *Una lettura comparatistica della L.675/96 sul trattamento dei dati personali*, in *Rivista trimestrale di diritto procedurale civile*, 1998, pp.733 ss.

valorizzazione della dignità umana e dell'autodeterminazione della singola persona, che nelle caratteristiche fondamentali[442], come l'indisponibilità, l'extrapatrimonialità e l'intrasmissibilità[443].

A differenza dei diritti della personalità, l'autonomia informativa richiede però una tutela preventiva che si concretizza in una serie di obblighi di comportamento posti in capo al responsabile del trattamento dati, come il dovere di informare l'interessato e di ottenere il suo consenso alla raccolta delle informazioni, che deve aver luogo indipendentemente da un'effettiva lesione subita dal soggetto stesso[444]. La tutela del diritto all'autonomia informativa non si limita inoltre a salvaguardare l'identità della persona, diventando una precondizione per l'esercizio di altre libertà fondamentali, come la libera espressione. Si può perciò affermare che la *data protection* svolge anche una funzione strumentale di interesse pubblicistico e gli strumenti di tutela giuridica devono tenere conto di questa peculiarità[445].

4. I principali strumenti legislativi internazionali a tutela del diritto alla protezione dei dati personali

I valori dell'autonomia informativa e della *data protection* rivestono un'importanza particolare nelle democrazie moderne: sono elementi imprescindibili per il mantenimento dell'ordine costituito e per permettere alle persone di raggiungere la propria autodeterminazione, sia sotto un profilo emotivo che intellettuale. Solo quando lo Stato riesce a garantire la privacy dei propri cittadini, questi sono liberi di esprimere la propria opinione senza timore di ripercussioni da parte degli altri membri della comunità e di prendere parte alla vita sociale e politica.

L'importanza di detti principi è ben esemplificata dai numerosi Trattati e documenti internazionali che nel corso degli anni hanno riconosciuto il valore fondamentale del diritto alla vita privata e all'autonomia informativa.

4.1. Il diritto all'autonomia informativa nel quadro giuridico delle Nazioni Unite

[442] Per un'analisi completa delle caratteristiche dei diritti della personalità nel contesto dell'informatica, si rimanda a V.ZENO-ZENCOVICH, *Profili negoziali degli attributi della personalità,* in *Diritto dell'informatica,* 1993, pp.545 ss.
[443] M.GAMBINI, *op.cit.*
[444] G.RESTA, *Il diritto alla protezione dei dati personali,* in (a cura di) F.CARDARELLI, S.SICA, V.ZENO-ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Milano, 2004, pp.11-64.
[445] M.GAMBINI, *op.cit.*

Le Nazioni Unite non riconoscono formalmente il carattere fondamentale del diritto all'autonomia informativa e alla *data protection*, sebbene il diritto alla privacy sia ormai una parte integrante ed ineludibile del diritto internazionale.

L'art.12 della Dichiarazione Universale dei Diritti Umani[446] afferma le prerogative dell'individuo a mantenere intatta la propria sfera privata, salvaguardando la propria vita intima e famigliare da intrusioni e ingerenze di terzi. Pur non avendo un valore vincolante, tale documento ha influenzato in maniera importante lo sviluppo del diritto internazionale successivo, specialmente per quanto riguarda la tutela dei diritti umani.

L'art.17 del Patto Internazionale sui Diritti Civili e Politici[447], approvato dall'Assemblea Generale ONU nel 1966, sancisce che nessuna persona deve veder sottoposta la propria vita privata a interferenze arbitrarie da parte di altri soggetti e la propria reputazione ad attacchi illegittimi. L'attenzione non è quindi rivolta esclusivamente a tutelare l'individuo da una possibile violazione "fisica" della propria dimensione privata, ma anche alla salvaguardia dell'onore e della rispettabilità nel contesto sociale. Si iniziano ad avere ben chiari i pericoli derivanti da una circolazione incontrollata delle informazioni, resa possibile dalle nuove tecnologie.

Questa consapevolezza ha portato l'Assemblea Generale delle Nazioni Unite a promulgare una prima risoluzione[448] nel 2014 in materia di diritto alla privacy nel contesto digitale; seppur non legalmente vincolanti, le parole dell'Assemblea hanno contribuito al dibattito in merito a questo tema e ad accendere l'attenzione globale sui pericoli che una sorveglianza massiva, condotta con la giustificazione dell'interesse nazionale, può avere per l'esercizio delle libertà fondamentali. Una successiva risoluzione[449], datata 2016, ha affrontato il medesimo tema da una prospettiva diversa, evidenziando che i rischi per la privacy delle persone possono arrivare anche dalla

---

[446] Assemblea Generale delle Nazioni Unite, Ris.219077A, 10 dicembre 1948, Dichiarazione Universale dei Diritti Umani, https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf (consultata il 16 luglio 2019).

[447] Assemblea Generale delle Nazioni Unite, Ris.14668, 19 dicembre 1966, Patto Internazionale sui Diritti Civili e Politici, https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf (consultato il 16 luglio 2019).

[448] Assemblea Generale delle Nazioni Unite, Ris. A/RES/68/167, *Il diritto alla privacy nell'era digitale*, 21 gennaio 2014, https://undocs.org/A/RES/68/167 (consultato il 16 luglio 2019).

[449] Assemblea Generale delle Nazioni Unite, Ris A/C.3/71/L39/Rev.1 https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1 (consultato il 16 luglio 2019).

raccolta di dati personali condotta da soggetti privati, come società e aziende, per finalità commerciali.

4.2. Il diritto alla privacy nell'art.8 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali

Il Consiglio di Europa è un Organizzazione Internazionale fondata a seguito della Seconda Guerra Mondiale per propagandare e proteggere i valori della democrazia e dello stato di diritto sul territorio europeo.

La Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali[450], ratificata nel 1950 ed entrata ufficialmente in vigore nel1953, persegue tale scopo. Gli Stati firmatari hanno l'obbligo di rispettare le previsioni della Convenzione, incorporandola o attribuendole valore legale attraverso apposite disposizioni legislative nazionali. La Corte Europea dei Diritti dell'Uomo ha il compito di sanzionare eventuali comportamenti contrari a quanto previsto dalla Carta, considerando i ricorsi di individui, gruppi di individui e persone giuridiche come ONG e associazioni internazionali. Possono agire di fronte alla Corte anche Stati che segnalano violazioni tenute da altri Paesi contraenti.

L'art.8 della Convenzione sancisce il diritto al rispetto della vita privata e familiare, della casa e della corrispondenza. La disposizione tutela due differenti valori della persona: da una parte il rispetto della vita privata che deve essere salvaguardata da intrusioni esterne, e dall'altra l'inviolabilità di un diverso tipo di spazio, quello emozionale e reputazionale, in cui l'essere umano deve sentirsi libero di formare ed esprimere la propria personalità[451].

La terminologia utilizzata nella formulazione dell'art.8 si distingue da quella degli altri articoli della Convenzione, poiché l'attenzione viene posta sul "rispetto" della dimensione intima della persona e non su un esplicito diritto alla privacy[452]. Questa

---

[450] Consiglio di Europa, Trattato n.005, *Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali*, 4 novembre 1950, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005 (consultato il 17 luglio 2019).

[451] B.M. HALE, *Countryside Alliance and others v Attorney General and another*, (2007) UKHL 52, par.110, https://publications.parliament.uk/pa/ld200708/ldjudgmt/jd071128/countr-1.htm (consultato il 17 luglio 2019), par.110.

[452] S.LAMBERT, A.LINDSAY-STURGO, *Focus on art.8 ECHR: recent developments*, in *Judicial Review*, n.13, 2008, pp.29 e ss.

particolare scelta terminologica, insieme alla specificazione che le limitazioni al libero esercizio di tale diritto sono consentite solamente se "*necessarie per una società democratica*"[453], ha lasciato un ampio margine di discrezionalità alla Corte Europea dei Diritti dell'Uomo nella valutazione della sussistenza di un'effettiva violazione dell'art.8.

L'articolo in questione è formulato secondo il tradizionale schema dell'obbligazione negativa[454]: il potere pubblico deve astenersi dall'interferire con la dimensione privata della persona, così come devono farlo gli altri membri della collettività. Lo Stato può però essere chiamato ad adottare misure concrete[455] per far sì che i propri cittadini godano di una vita intima senza dover temere ingerenza alcuna; spetta perciò alla Corte valutare quali siano gli effettivi doveri dello Stato nel caso in esame.

Per determinare se una specifica limitazione del diritto sancito dall'art.8 può essere considerata come necessaria per il mantenimento dell'ordine democratico, i giudici di Strasburgo devono trovare un punto di equilibrio tra gli interessi dello Stato e quelli del ricorrente. Un orientamento giurisprudenziale più risalente vedeva come legittima l'interferenza apportata dal potere pubblico alla dimensione privata di un individuo se era necessaria per rispondere a un pressante bisogno dell'intera collettività sociale[456]; spettava allo Stato chiamato in causa giustificare tale requisito. Successivamente la Corte ha affermato che per essere considerata necessaria per la salvaguardia della democrazia, un'ingerenza alla privacy doveva essere considerata come proporzionata alle finalità, che dovevano essere comunque compatibili con la CEDU, che intendeva perseguire[457]. Per poter valutare se il criterio di proporzionalità è stato effettivamente rispettato, i giudici devono primariamente esaminare le scelte legislative che sono alla base della misura intrapresa e oggetto di controversia; in questa maniera è possibile stabilire se i diritti della persona sono stati effettivamente rispettati e se questa ha rispettato i criteri di ammissibilità del ricorso alla Corte, come il previo esperimento dei mezzi di tutela giurisdizionale interni.

---

[453] Art.8 par.2 della Convenzione Europea sulla salvaguardia dei Diritti Umani e delle Libertà Fondamentali.
[454] Corte Europea dei Diritti dell'Uomo, *Kroon and Others v.Netherlands,* ricorso n.18535/91, 27 ottobre 1994, par.31.
[455] Corte Europea dei Diritti dell'Uomo, *Lozovyye v.Russia*, ricorso n. 4587/09, 24 luglio 2018, par.36.
[456] Corte Europea dei Diritti dell'Uomo, *Dudgeon v.The United Kingdom*, ricorso n.7525/76, 22 ottobre 1981, par.51-53.
[457] Corte Europea dei Diritti dell'Uomo, *Z v. Finland,* ricorso n.22009/93, 25 febbraio 1997, par.94.

4.2.1. La definizione di "vita privata" e il diritto alla protezione dei dati personali nella giurisprudenza della Corte Europea dei Diritti dell'Uomo

Il concetto di "vita privata" è ampio e difficilmente racchiudibile in un'unica definizione, poiché abbraccia diversi aspetti della socialità di una persona[458]. Non indica solamente una dimensione che è prerogativa esclusiva della persona, nella quale è precluso l'ingresso per ogni altro soggetto terzo e che non ha collegamenti con il mondo circostante. L'art.8 della Convenzione protegge il diritto all'autonomia personale, garantendo agli individui di entrare in contatto con gli altri membri della collettività e di intrattenere con loro relazioni di ogni tipo; è il diritto ad avere una "vita sociale privata"[459]. Può includere ciò che avviene durante l'espletamento di attività professionali[460] o commerciali, così come le interazioni con altre persone avvenute in luogo pubblico[461].

La raccolta e il trattamento di dati personali da parte di una pubblica autorità possono comportare la violazione di quanto previsto dall'art.8, specialmente se le informazioni raccolte fanno riferimento al lontano passato della persona a cui si riferiscono[462] o alle sue opinioni politiche e ideologiche, ricadendo quindi nella categoria dei dati sensibili e maggiormente bisognosi di un'adeguata tutela[463].

La Corte Europea dei Diritti dell'Uomo si è trovata in numerose occasioni a dover valutare l'effettiva sussistenza di una violazione dell'art.8, sviluppando una casistica di cui si vuole compiere una breve rassegna non esaustiva. Ad esempio, sono stati sanzionati comportamenti abusivi nel caso di informazioni personali relative alle idee politiche raccolte e archiviate da autorità pubbliche[464], così come nell'inclusione di nominativi all'interno di archivi nazionali di persone colpevoli di crimini sessuali[465]. I giudici di

[458] Corte Europea dei Diritti dell'Uomo, *S and Marper v. The United Kingdom,* ricorsi riuniti n.30562/04 e n.30566/04, 4 dicembre 2008, par.66.
[459] Corte Europea dei Diritti dell'Uomo, *Barbulescu v.Romania,* ricorso n.61496/08, 5 settembre 2017, par.71; Corte Europea dei Diritti dell'Uomo, *Botta v.Italy,* ricorso n. 153/1996/772/973, 24 febbraio 1998, par.32.
[460] Corte Europea dei Diritti dell'Uomo, *Fernandez Martinez v.Spain,* ricorso 56030/07, 12 giugno 2014, par.110.
[461] Corte Europea dei Diritti dell'Uomo, *Uzun v.Germany,* ricorso 35623/05, 2 dicembre 2010, par.43.
[462] Corte Europea dei Diritti dell'Uomo, *Rotaru v.Romania,* ricorso 28341/95, 4 maggio 2000, par.43-44.
[463] Corte Europea dei Diritti dell'Uomo, *Catt v.The United Kingdom*, ricorso 43514/15, 24 aprile 2019, par.112 e 123.
[464] Corte Europea dei Diritti dell'Uomo, *Associazione "21 dicembre 1989" and others v.Romania,* ricorso n.33810/07, 24 maggio 2011, par.115.
[465] Corte Europea dei Diritti dell'Uomo, *Gardel v.France,* ricorso 16428/05, 17 marzo 2010, par.58.

Strasburgo hanno ritenuto violato l'art.8 anche in mancanza delle opportune tutele giuridiche per la raccolta e il trattamento delle impronte digitali delle persone imputate di reato (ma non ancora condannate)[466] e nella richiesta agli atleti professionisti di fornire a cadenza regolare informazioni sulla loro posizione geografica e sulle loro attività nell'ambito della lotta al doping[467].

La Corte non ha invece rilevato alcuna violazione da parte dello Stato che collaziona dati personali di soggetti arrestati per atti terroristici[468]; le autorità pubbliche non possono però ricorrere ad ampie e indiscriminate operazioni di raccolta informazioni di soggetti imputati di reato senza una chiara e dettagliata legittimazione normativa che preveda le adeguate garanzie anche per le persone coinvolte[469].

Le pronunce della Corte Europea dei Diritti dell'Uomo qui prese in considerazione offrono lo spunto per alcune considerazioni. Non è possibile ricostruire in maniera aprioristica le caratteristiche di una condotta in violazione del diritto al rispetto della vita familiare e privata così come riconosciuto dall'art.8 della Convenzione; le numerose circostanze ed evenienze in cui questa può verificarsi impediscono qualsiasi elenco tassativo.

Il diritto alla privacy entra in gioco in moltissimi aspetti della vita quotidiana che non possono essere riassunti preventivamente in un articolo della Convenzione, anche alla luce del costante progresso tecnologico che causa sempre nuovi rischi per la sfera privata e intima delle persone. La Corte deve inoltre mantenere un delicato equilibrio tra interessi apparentemente contrapposti: da una parte la necessità degli Stati di mantenere la sicurezza all'interno del territorio nazionale, obbiettivo spesso raggiunto anche attraverso operazioni di raccolta dati e di sorveglianza digitale, dall'altra parte il diritto dei cittadini alla tutela della propria privacy e autonomia informativa contro l'intervento dei pubblici poteri. I giudici devono quindi esercitare il proprio potere discrezionale valutando caso per caso le circostanze che sono portate alla loro attenzione: questo è reso possibile anche dalla formulazione stessa dell'art.8, che si distingue per la sua ampiezza e non tassatività.

---

[466] Corte Europea dei Diritti dell'Uomo, *M.K.v.France,* ricorso 19522/09, 18 luglio 2013, par.26.
[467] Corte Europea dei Diritti dell'Uomo, *National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*, ricorsi uniti n.48151/11 e 77769/13, 18 aprile 2018, par.155-159.
[468] Corte Europea dei Diritti dell'Uomo, *Murray v. The United Kingdom,* ricorso n.14310/88, 28 ottobre 1994, par.93.
[469] Corte Europea dei Diritti dell'Uomo, *M.M. v. The United Kingdom,* ricorso n.24029/07, 29 aprile 2013, par.199.

4.3. La Convenzione 108 del Consiglio di Europa: il primo documento internazionale in materia di trattamento automatico dei dati

La Convenzione Europea sulla salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali risale, come già accennato, al 1950, quando l'evoluzione delle reti digitali stava appena compiendo i primi passi. Negli anni successivi si è avvertita l'esigenza di rinnovare la protezione giuridica riconosciuta alla condivisione dei dati aggiornandola all'avvenuto progresso tecnologico; il Comitato dei Ministri del Consiglio di Europa ha perciò adottato diverse risoluzioni[470] in materia, mantenendo comunque la base dell'art.8 della Convenzione.

Un ulteriore passo in avanti è stato fatto con la Convenzione 108 per la protezione degli individui nei confronti del trattamento automatico dei dati personali[471]; rimane allo stato attuale l'unico atto internazionale vincolante nell'ambito di tutela dell'autonomia informativa e della *data protection*. Quanto previsto dalla Convenzione 108 si applica a ogni tipo e modalità di raccolta e gestione delle informazioni, indipendentemente da chi ne è il diretto responsabile; sono quindi sottoposti a tale disciplina sia i soggetti privati che pubblici, compresi i trattamenti svolti dalle autorità giudiziarie e dalle forze di polizia. Lo scopo della Convenzione è proteggere i soggetti coinvolti da ogni possibile abuso riguardante l'utilizzo dei loro dati stabilendo i principi da seguire categoricamente per il loro trattamento come il rispetto delle modalità e delle finalità previste al momento della raccolta.

Le informazioni non devono essere perciò utilizzate per scopi difformi da quelli preventivamente comunicati e devono essere correttamente cancellate una volta esaurita la loro necessità; il soggetto coinvolto mantiene il diritto di accedere alle informazioni che lo riguardano, potendo modificarne il contenuto nel modo che ritiene più opportuno.

La Convenzione stabilisce inoltre un divieto generale di raccolta e gestione di dati attinenti a profili particolarmente sensibili della personalità umana, come la sua identità sessuale e di genere, le sue ideologie politiche o il suo credo religioso; tale divieto è

[470] Comitato dei Ministri del Consiglio di Europa, risoluzione (73) 22, *Resolution on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector*, 26 settembre 1973; Comitato dei Ministri del Consiglio di Europa, risoluzione (74) 29, *Resolution on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector*, 20 settembre 1974.

[471] Convenzione per la protezione degli individui nei confronti del trattamento automatico dei dati personali, CETS n.108, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181 (consultato il 18 luglio 2019).

superabile solo nell'ottica di un interesse superiore che va a vantaggio dell'intera collettività.

Le reti digitali hanno raggiunto una dimensione globale, oltrepassando i tradizionali confini giuridici e politici e permettendo una continua condivisione di dati personali; un ulteriore scopo della Convenzione è proprio quello di permettere che tali scambi di informazioni avvengano nel pieno rispetto dei diritti fondamentali delle persone coinvolte. A tal proposito sono consentite liberamente le trasmissioni di dati tra i Paesi firmatari, mentre vengono previsti requisiti ulteriori per quelle dirette verso Stati non facenti parte della Convenzione e i cui ordinamenti non prevedono una tutela ritenuta equivalente.

La Corte Europea dei Diritti dell'Uomo, pur non avendo competenza a svolgere un sindacato giurisdizionale sulla sua corretta applicazione, ha fatto riferimento numerose volte alla Convenzione 108 nelle sue sentenze, stabilendo che la *data protection* è un aspetto fondamentale del diritto al rispetto della vita privata[472].

Data la sua apertura alla ratifica da parte di Stati non facenti parte del Consiglio di Europa, la Convenzione può affermarsi come uno standard universale per la tutela del diritto all'autonomia informativa; hanno ratificato questo documento tutti i Paesi membri dell'Unione Europea, ma anche Nazioni sudamericane come l'Uruguay o africane come la Tunisia e il Senegal, per un totale attuale di 51 parti contraenti.

4.4. Il diritto alla privacy e all'autonomia informativa nell'ordinamento dell'Unione europea

La tutela della privacy e la salvaguardia della *data protection* sono principi essenziali per l'azione dell'Unione europea mirata all'integrazione economica del continente e al mantenimento della pace e della concordia tra gli Stati membri. Tali valori sono infatti essenziali per lo sviluppo dell'ordine democratico: un cittadino può sentirsi effettivamente libero di esprimere la propria opinione solamente se non deve temere ingerenze nella propria sfera privata.

Il Preambolo del Trattato all'Unione europea afferma l'importanza dei principi della democrazia, della *Rule of law* e del rispetto dei diritti fondamentali: l'art.2 del medesimo Trattato prosegue sulla stessa linea impegnando gli Stati membri a seguire detti

[472] Corte Europea dei Diritti dell'Uomo, *Z v. Finland,* ricorso n.22009/93, 25 febbraio 1997, par.94.

principi nel corso della loro azione politica e normativa. Viene attribuita a questi principi una valenza universale (art.21 TUE) che deve guidare l'operato stesso dell'Unione europea.

4.5. Il diritto alla tutela dei dati personali nei Trattati istitutivi dell'Unione europea

Il Trattato istitutivo delle Comunità europee non conteneva alcun riferimento ai diritti fondamentali e alla loro protezione: la Comunità Economica Europea era infatti nata come un'organizzazione regionale di integrazione economica, con lo scopo di promuovere un mercato unico tra i propri membri.

La proclamazione della Carta dei Diritti Fondamentali dell'Unione europea[473] (d'ora in poi anche "la Carta") segna perciò un importante cambio di prospettiva; questo documento elenca i diritti economici, politici, sociali e civili dei cittadini europei, frutto di un'elaborazione complessiva e sintetica delle tradizioni costituzionali dei Paesi membri. Originariamente inteso come un documento dal valore esclusivamente politico, la Carta è diventata legalmente vincolante con l'approvazione del cd.Trattato di Lisbona del 2009; l'art.6.1 del TUE[474] le riconosce infatti lo stesso valore giuridico dei Trattati, elevandola al rango di diritto primario dell'Unione europea. Le Istituzioni europee sono perciò tenute a rispettare le previsioni della Carta nello svolgimento delle loro azioni, così come devono fare gli Stati membri nell'esecuzione e implementazione della normativa dell'Unione europea.

Viene riconosciuto al diritto all'autodeterminazione informativa e alla *data protection* un valore fondamentale (art.8.1) e non di mero corollario al più generale diritto alla privacy. La Carta stabilisce inoltre i principi di legittimità secondo i quali deve essere condotto ogni trattamento di dati personali (art.8.2): tali informazioni devono essere gestite secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Si riconosce infine la necessità di un'Autorità *super partes* e indipendente che vigili

[473] Carta dei Diritti Fondamentali dell'Unione europea, in GU C 326, 26 ottobre 2012, pp.391-407, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:12012P/TXT (consultato il 24 luglio 2019).
[474] Trattato sull'Unione europea (versione consolidata) in GU C 326, 26 ottobre 2012, pp.13-390, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX%3A12012M%2FTXT (consultato il 24 luglio 2019).

sull'effettivo rispetto dei diritti fondamentali delle persone coinvolte nella trasmissione dei dati personali (art.8.3).

Il Trattato di Lisbona ha portato un'ulteriore innovazione meritevole di menzione: una nuova base giuridica per l'azione dell'Unione Europea nella tutela del diritto alla protezione dei dati personali. La normativa previgente in materia era stata infatti adottata con lo scopo di favorire lo stabilimento del mercato unico europeo, garantendo il flusso di dati tra i vari Stati membri. L'art.16 del TFUE[475] afferma che ogni persona ha il diritto alla protezione dei dati personali che la riguardano impegnando l'Unione europea ad agire affinché tale diritto venga effettivamente garantito in quanto tale, e non per raggiungere una finalità ulteriore e diversa.

4.6. *Dalla direttiva 95/46/CE al Regolamento (UE) 2016/679: l'evoluzione normativa europea nella tutela dei dati personali*

La direttiva 95/46/CE[476] ha segnato senza dubbio un punto di svolta per la tutela dei dati personali sul territorio europeo, rappresentando il primo tentativo dell'allora Comunità europea di dotarsi di una disciplina in tale ambito valevole per ogni Paese membro. L'utilizzo dello strumento legislativo della direttiva richiedeva perciò a ogni Stato di armonizzare le proprie normative con l'obbiettivo di una più uniforme applicazione e una più omogenea interpretazione a livello europeo, rispettando i principi minimi inderogabili elencati dalla direttiva stessa. Valori quali la liceità del trattamento e la qualità dei dati, il diritto di accesso e modifica delle informazioni condivise, il consenso libero e informato entrano nella legislazione a tutela dei dati personali formulata dagli Stati nazionali.

La naturale flessibilità della direttiva ha fatto sì che la normativa fosse in grado di adattarsi a numerose esigenze, spesso differenti rispetto a quelle per cui era originariamente programmata. Questa caratteristica si è però dimostrata essere anche una profonda debolezza che ha spinto i legislatori a valutare una modifica della disciplina in questione: il costante progresso tecnologico, impensabile al momento dell'emanazione

[475] Trattato sul funzionamento dell'Unione europea (versione consolidata) in GU C 326, 26 ottobre 2012, pp.47-390, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A12012E%2FTXT (consultato il 24 luglio 2019).
[476] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in GU L 281, 23 novembre 1995, pp.31-50.

della direttiva, ha costretto la Corte di giustizia dell'Unione europea a un costante sforzo interpretativo ed esegetico per adattare la regolamentazione in esame alle esigenze di una società digitale in continuo mutamento.

Partendo da questa consapevolezza, le successive direttive 2002/58/CE[477] e 2006/24/CE[478] hanno svolto una funzione integrativa[479] di quanto già disposto dalla direttiva 95/46/CE rafforzandone e ampliandone il nucleo centrale[480] sotto molteplici aspetti. Hanno portato a un sostanziale ammodernamento della disciplina legislativa in tema di telecomunicazioni, specificando inoltre in maniera dettagliata le prerogative dell'intero apparato di controllo già predisposto dalla normativa del'95.

La direttiva 2002/58/CE ha l'obbiettivo di regolamentare la condivisione dei dati personali attraverso le comunicazioni elettroniche rispettando i diritti e le prerogative dell'utente cibernetico; consapevole dell'impatto dirompente di Internet e delle reti digitali nel mondo della comunicazione, il legislatore europeo ha introdotto termini come *web bugs*[481] e *cookies*[482], ancora impensabili nel 1995.

Andando ad osservare le misure più importanti introdotte con la direttiva del 2002, si nota che l'art.4 impone al fornitore di servizi di comunicazione elettronica accessibili al pubblico di prevedere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dell'utente finale. Per raggiungere tale obbiettivo, può collaborare con il

---

[477] 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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche), in GU L201, 31 luglio 2002, pp. 37-47.

[478] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, in GU L 105, 13 aprile 2006, pp.54-63.

[479] L'art.1.2 della direttiva 2002/58/CE specifica che "*le disposizioni della presente Direttiva precisano e integrano la Direttiva 95/46/CE*".

[480] F.PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, pp.136.

[481] Considerando n.24 della direttiva 2002/58/CE recita "[…] *I cosiddetti software spia, bachi invisibili ("web bugs"), identificatori occulti ed altri dispositivi analoghi possono introdursi nel terminale dell'utente a sua insaputa al fine di avere accesso ad informazioni, archiviare informazioni occulte o seguire le attività dell'utente e possono costituire una grave intrusione nella vita privata di tale utente. L'uso di tali dispositivi dovrebbe essere consentito unicamente per scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza"*.

[482] Considerando n.25 della direttiva 2002/58/CE recita "[…] *i cosiddetti marcatori ("cookies"), possono rappresentare uno strumento legittimo e utile, per esempio per l'analisi dell'efficacia della progettazione di siti web e della pubblicità, nonché per verificare l'identità di utenti che effettuano transazioni "on-line". Allorché tali dispositivi, ad esempio i marcatori ("cookies"), sono destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, il loro uso dovrebbe essere consentito purché siano fornite agli utenti informazioni chiare e precise, a norma della direttiva 95/46/CE, sugli scopi dei marcatori o di dispositivi analoghi per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando. Gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore o un dispositivo analogo sia installato nella loro apparecchiatura terminale* […]".

fornitore della rete pubblica utilizzata. L'art.5 impone agli Stati un divieto di captare e intercettare informazioni e comunicazioni avvenute sulle reti elettroniche, a meno che non sia necessario per esigenze di ordine pubblico. Secondo l'art.15, l'utente deve essere inoltre costantemente aggiornato sulle modalità di trattamento dei propri dati personali attraverso apposite informative, in maniera tale che possa eventualmente rifiutare il suo consenso alla raccolta dei dati che lo riguardano. La direttiva 2002/58/CE elenca determinati principi che andranno a costituire la "spina dorsale" della disciplina normativa europea in tema di *data protection* e che verranno ripresi anche dalla legislazione successiva; si pensi al principio della finalità (art.6), per cui le informazioni non più necessarie al perseguimento degli scopi del trattamento dati devono essere immediatamente cancellate, e al valore dell'anonimizzazione (art.7), secondo il quale i dati trattati devono essere gestiti in maniera tale da far sì che il soggetto a cui si riferiscono non sia identificabile se non nelle eventualità strettamente necessarie.

La direttiva 2006/24/CE si concentrava su un tema particolarmente specifico, volendo disciplinare le modalità di conservazione dei dati personali e il loro utilizzo per finalità di indagine per reati particolarmente gravi. Una delle motivazioni di questa volontà legislativa è data dai tragici attacchi terroristici avvenuti nella città di Londra nel 2005[483]: l'esigenza di un'immediata risposta delle forze di polizia in simili occasioni può infatti portare a dover raccogliere grandi quantità di informazioni. L'interesse pubblico e la necessità di mantenere la sicurezza all'interno dei territori nazionali non possono essere però motivazioni per abusare del diritto alla privacy e alla tutela dei dati personali. La creazione di una disciplina comune che armonizzasse le diverse disposizioni nazionali e che tenesse conto dei diversi interessi in gioco si era perciò fatta ineludibile.

L'art.6 della direttiva 2006/24/CE prevedeva un tempo minimo (6 mesi) e un periodo massimo (2 anni) di conservazione da parte dei pubblici poteri di particolari dati relativi alle comunicazioni elettroniche: l'interpretazione e applicazione di questo specifico articolo è stata oggetto di un rinvio pregiudiziale [484] alla Corte di giustizia dell'Unione europea.

I giudici hanno rilevato che i dati in questione, pur non attenendo specificatamente al contenuto delle comunicazioni stesse, possono rivelare comunque aspetti importanti

[483] Il considerando n.10 della direttiva in questione fa esplicito riferimento agli attacchi terroristici avvenuti a Londra nel 2005, esprimendo una ferma condanna di tali attentati da parte dell'intera Europa.
[484] Corte di giustizia dell'Unione europea, casi riuniti C-293/12 e C-594/12, *Digital Rights Ireland v. Minister of Communications and others,* sentenza dell'8 aprile 2014.

relative alle conversazioni, alla loro frequenza e alle parti coinvolte, comportando perciò un serio pregiudizio per il diritto alla privacy e alla riservatezza delle persone. La Corte ha inoltre segnalato una violazione del principio di proporzionalità del trattamento dati per 5 diversi motivi[485]:

1) Non aver previsto termini specifici per la conservazione dei dati raccolti a seconda delle diverse circostanze e dei diversi casi concreti;
2) Non aver adeguatamente specificato cosa si intende per "reati gravi";
3) aver omesso ogni presupposto procedurale e sostanziale al quale subordinare l'accesso;
4) Aver previsto esclusivamente i termini massimi e minimi di conservazione delle informazioni;
5) Non aver stabilito che i dati devono essere conservati all'interno del territorio dell'Unione europea.

I giudici della Corte di giustizia hanno quindi preso la decisione di annullare la direttiva in questione, ritenendo che la mancanza di specificazione e differenziazione normativa in un campo particolarmente delicato come quello della *data protection* potesse causare un grave pregiudizio alla sfera privata dei cittadini europei. Una limitazione dei diritti fondamentali può essere infatti considerata legittima esclusivamente se proporzionata alle esigenze di pubblica sicurezza perseguite: tale criterio di proporzionalità non può essere definito in maniera aprioristica ed astratta, ma deve essere parametrato alle circostanze del caso concreto, specialmente in un ambito come quello della lotta al crimine che può fare da preludio a eventuali abusi.

Questa breve panoramica sulla normativa più risalente in tema di protezione dei dati personali risulta indispensabile per poter affrontare con cognizione di causa lo studio del Regolamento (UE) 2016/679[486], chiamato anche GDPR, recentemente entrato in vigore nell'ordinamento europeo e che abroga interamente la previgente direttiva 95/46/CE. Era infatti ormai diffusa l'esigenza di una nuova disciplina uniforme in tema di *data protection* che potesse rispondere in maniera adeguata agli importanti cambiamenti apportati dal costante progresso tecnologico.

---

[485] Per un'attenta analisi della sentenza *Digital Ireland* e delle sue conseguenze giuridiche, si rimanda a F.M.DONNINI, *L'evoluzione della protezione dei dati personali tra tecnologia, sicurezza nazionale e diritti fondamentali*, Roma, 2017, pp.77 ss.

[486] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in GU L 119, 4 maggio 2016, pp. 1-88.

5. Il Regolamento (UE) 2016/679 (GDPR) e la tutela dei dati personali nell'epoca digitale

L'entrata in vigore del Regolamento (UE) 2016/679 è un momento cardine dell'evoluzione normativa in materia di tutela dei dati personali per diversi motivi.

A differenza di quanto accaduto con la direttiva 95/46/CE, viene utilizzato lo strumento legislativo del Regolamento; l'intento non è più quello di avvicinare e armonizzare diverse disposizioni normative nazionali, frutto anche di differenti culture giuridiche, ma di proporre una disciplina immediatamente vincolante per tutto il territorio europeo e che non richieda una costante opera di interpretazione da parte della Corte di giustizia dell'Unione europea. La flessibilità della direttiva 95/46/CE aveva sì permesso di rispondere velocemente a diverse esigenze e problematiche che non erano neppure immaginabili al tempo dell'entrata in vigore della normativa stessa, ma aveva anche lasciato spazio a un differente recepimento della direttiva da parte dei diversi Stati membri. La diversa legislazione in materia rischiava di non offrire una tutela uniforme su tutto il territorio europeo per il trattamento dei dati personali dei soggetti coinvolti e questa era una situazione non più accettabile in una società globalmente connessa, dove le informazioni viaggiano in tempo reale indipendentemente dai confini giuridici e dagli ordinamenti legislativi.

Non bisogna però credere che il GDPR si ponga in una sostanziale posizione di rottura nei confronti della normativa previgente, poiché recepisce i principi fondamentali della direttiva 95/46/CE per adattarli e applicarli in maniera ancora più efficace in un contesto sociale ed economico completamente differente rispetto a quello in cui aveva visto la luce la direttiva ora abrogata.

Il Regolamento (UE) 2016/679 deve trovare un difficile punto di equilibrio tra due spinte apparentemente antitetiche[487]; da una parte deve essere caratterizzato da una semplicità di impianto che ne possa garantire un'interpretazione elastica, adattabile anche a circostanze non ancora attuali, ma comunque preventivabili per la costante evoluzione tecnologica, e dall'altra deve stabilire un nucleo fondante di principi e valori fondamentali che non possa essere scalfito dalla diversità delle legislazioni nazionali dei Paesi membri dell'Unione europea.

[487] F.M.DONNINI, *op.cit.*

Questa contrapposizione si rispecchia nel testo del Regolamento, che si presenta infatti come una normativa di dettaglio commista a definizioni giuridiche elastiche e flessibili[488]. Un simile approccio ha però mostrato il fianco ad alcune osservazioni critiche: il carattere rigido di alcune disposizioni, forse più assimilabili a dichiarazioni di principio che a previsioni normative[489], rischia di limitarne la flessibilità e l'applicazione, mentre la natura più generale di altre fa sì che la prassi applicativa degli Stati possa mostrarsi difforme e non coerente.

Il rischio di un'applicazione non uniforme da parte dei Paesi membri dell'Unione europea di quanto previsto dal Regolamento (UE) 2016/679 dovrebbe essere scongiurato dalla lunga normativa di dettaglio che il GDPR prevede per regolamentare il comportamento dei soggetti coinvolti nel trattamento dati. Si assiste a un sostanziale cambio di prospettiva[490] rispetto all'approccio utilizzato dall'ormai abrogata direttiva 95/46/CE, che poneva il rispetto dei diritti delle persone interessate dal trattamento al centro della tutela giurisdizionale; la tutela di tali diritti è ora garantita principalmente da un'attenta e pedissequa regolamentazione delle azioni degli operatori del settore. Fino a quando questi si manterranno all'interno del sentiero regolamentare tracciato dal GDPR, le persone coinvolte non dovranno temere alcunché in merito alla protezione delle informazioni che le riguardano.

5.1. La definizione di "dato personale" fornita dal Regolamento (UE) 2016/679

La definizione di "dato personale" fornita dal GDPR è un efficace esempio della attenzione al dettaglio normativo che caratterizza tutto il testo del Regolamento (UE) 2016/679.

L'art.4, seguendo quanto previsto dalla previgente direttiva 95/46/CE, descrive il "dato personale" come l'informazione che identifica o rende identificabile il soggetto a cui si riferisce. L'elemento di novità si coglie nel dettagliato elenco di identificativi fornito dal medesimo articolo, nel tentativo di tenere il passo dell'evoluzione tecnologica. Il GDPR inserisce infatti tra gli aspetti idonei a identificare una persona anche quelli frutto del progresso digitale; si pensi alla localizzazione geografica data dagli apparecchi GPS,

[488] S.SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali*, Cap.I, in (a cura di) S.SICA, V.D'ANTONIO, G.M.RICCIO, *La nuova disciplina europea della privacy,* Milano, 2016, pp.5 ss.
[489] F.PIZZETTI, *op.cit.*
[490] F.M.DONNINI, *op.cit.*

ai *cookie*, ossia stringhe di codice informatico utilizzate per individuare l'utente cibernetico a cui sono collegate e all'indirizzo IP.

Il Regolamento introduce tre diverse categorie di dati personali, non esplicitati chiaramente dalla previgente normativa: i dati genetici, sanitari e biometrici. I primi fanno riferimento alle caratteristiche ereditarie e genetiche dell'interessato, fornendo informazioni univoche sulla sua persona, anche attraverso l'analisi di campioni biologici. Gli elementi che indicano la condizione fisica e lo stato di salute di un individuo, comprensivi dei trattamenti medici a cui si è sottoposto, rientrano invece nella categoria dei dati sanitari. Per quanto riguarda i cd. dati biometrici, l'art.4 par.1 n.14 del Regolamento indica con tale parola le caratteristiche specifiche di una persona, individuabili attraverso trattamenti automatici specifici come la scansione dell'iride o la raccolta delle impronte digitali.

Pur apprezzando il livello di precisione offerto dalla definizione di "dato personale" fornita dal GDPR, rimane ancora apparentemente irrisolta la questione relativa ai cd. metadati: con tale termine si vogliono indicare "le informazioni sulle informazioni", ossia i dati che fanno riferimento non direttamente a un soggetto specifico, ma ad altre informazioni. Si pensi ad esempio al luogo di connessione di un utente allo spazio cibernetico, alla durata della sua navigazione sul *web* o alle parole inserite su un motore di ricerca: queste informazioni non sono generalmente di per sé idonee a identificare una persona, non rientrando quindi nell'ambito di applicazione della definizione di cui all'art.4 GDPR, ma sono comunque in grado di rivelarne caratteristiche importanti. Bisogna inoltre aggiungere che, qualora due o più metadati venissero combinati insieme, sarebbero probabilmente in grado di individuare in maniera esatta il soggetto a cui si riferiscono.

Spetterà probabilmente alla Corte di giustizia dell'Unione europea attraverso la sua opera di interpretazione valutare se le previsioni del Regolamento (UE) 2016/679 possono trovare applicazione anche per quanto riguarda la raccolta e il trattamento dei cd. metadati.

5.2. Trattamento, profilazione e pseudonimizzazione: la raccolta e la gestione dei dati personali secondo il Regolamento (UE) 2016/679

Il Regolamento (UE) 2016/679 propone una definizione aperta e non tassativa di "trattamento dati" che non venga resa obsoleta dal passare del tempo e che possa adattarsi

agli inevitabili cambiamenti tecnologici[491]. L'art.4.2 del GDPR indica con tale terminologia qualsiasi operazione condotta su dati personali; è indifferente che venga portata avanti *in toto* attraverso strumenti informatici o con l'ausilio dell'intervento umano.

Per quanto riguarda i soggetti attivamente coinvolti nella gestione delle informazioni, il "titolare" è colui che stabilisce gli scopi e le modalità del trattamento dati (art.4.7 GDPR) mentre il "responsabile" è l'entità concretamente incaricata di portare avanti la raccolta delle informazioni e la loro successiva lavorazione (art.4.8 GDPR).

L'attenzione prestata dal Regolamento (UE) 2016/679 alle nuove necessità della società digitale è testimoniata dalle innovative definizioni di "profilazione" (art.4.4. GDPR) e "pseudonimizzazione (art.4.5 GDPR).

Il primo termine indica «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*». Questo particolare tipo di trattamento consiste nella raccolta e analisi di un grande quantitativo di informazioni allo scopo di creare una sorta di "profilo digitale" degli utenti cibernetici per finalità commerciali. Comprendere i gusti e gli interessi di potenziali clienti permette infatti alle aziende che ricorrono alle attività di profilazione di generare ingenti guadagni, offrendo ai consumatori beni e servizi delineati sulle loro esigenze. Il rovescio della medaglia di queste modalità di trattamento è evidente: ci sono profili di rischio per la privacy degli interessati dalla raccolta delle informazioni che potrebbero essere sottoposti a una continua opera di controllo e sorveglianza, e per la loro autonomia decisionale che verrebbe compromessa indirettamente dall'opera di profilazione.

La "pseudonimizzazione" indica invece quel particolare tipo di trattamento dati che impedisce di attribuire le informazioni raccolte a uno specifico soggetto. Secondo il principio di finalità, una volta raggiunto lo scopo prefissato per l'utilizzo dei dati in questione questi dovrebbero essere cancellati, resi anonimi oppure "pseudonimizzati", intendendo con tale termine le tecniche di modifica e alterazione dei principali

[491] Considerando n.21 del Regolamento (UE) 2016/679.

identificativi in maniera tale che questi non possano più indicare la persona a cui si riferiscono.

5.3. I criteri di applicazione materiale e territoriale del Regolamento 2016/679 e i profili innovativi rispetto alla normativa previgente

Il Regolamento 2016/679 segna un deciso cambio di prospettiva da parte del legislatore europeo rispetto al suo atteggiamento precedente: la decisione di utilizzare, invece della direttiva, lo strumento legislativo del Regolamento, immediatamente applicabile e con efficacia diretta in ogni sua parte per gli Stati membri, non è certamente priva di conseguenze. La definizione precisa e marcata degli ambiti di applicazione materiale e territoriale del GDPR si è perciò rivelata un'esigenza imprescindibile che non poteva essere ovviamente lasciata allo sforzo normativo dei vari Paesi dell'Unione europea.

Il nuovo Regolamento, come la previgente direttiva 95/46, continua ad applicarsi a ogni raccolta di informazioni e a ogni trattamento di dati personali[492]. Sono pressoché identiche a quelle riportate dall'abrogata direttiva anche le cause di esclusione: il GDPR non si applica infatti a quei trattamenti dati che esulano dal campo di applicazione della normativa europea, quando si fa riferimento ad attività dei pubblici poteri condotte nell'ambito del Titolo V, capo II, TUE (Disposizioni Specifiche sulla Politica Estera e di Sicurezza Comune) o quando si tratta di azioni a carattere penale, come la salvaguardia della pubblica sicurezza. Un'ulteriore causa di esclusione si ha nel caso di un trattamento di dati personali effettuato da persone fisiche con finalità esclusivamente personali e domestiche. Il Considerando 18 del Regolamento 2016/679 porta a tal proposito l'esempio dei *social networks*, specificando però che «*il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.*».

Per quanto riguarda l'ambito di applicazione territoriale, si assiste invece a una radicale innovazione rispetto a quanto previsto dalla previgente direttiva, che limitava il proprio funzionamento alle attività di trattamento dati svolte/espletate all'interno del territorio di uno Stato membro dell'Unione europea, o dello Spazio Economico Europeo (SEE). Una simile previsione normativa si è ben presto rivelata inidonea a rispondere alle

[492] F.M.DONNINI, *op.cit.*

sfide lanciate da una società sempre più interconnessa a livello globale. Le attività di aziende informatiche con sede negli Stati Uniti, si pensi a Google o Facebook a mero titolo di esempio, avrebbero infatti potuto evitare l'applicazione della normativa in questione, posto che l'unico criterio determinante era il luogo fisico in cui venivano trattati i dati, non rilevando in alcun modo parametri alternativi quali la cittadinanza del soggetto interessato dal trattamento o la sua residenza abituale.

Il cd. criterio dello stabilimento rimane determinante anche nel Regolamento 2016/679, seppur da una prospettiva diversa, poiché l'art.3.1 del GDPR stabilisce che tale normativa «*si applica al trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.*».

Il legislatore dell'Unione ha quindi recepito le osservazioni sollevate dall'operato della Corte di giustizia, segnatamente dalla celebre sentenza *Google Spain* in cui viene proposta una nozione prettamente sostanziale del concetto di "stabilimento" secondo la quale "*occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni dei servizi in questione*" per determinare l'effettiva esistenza di uno stabilimento in uno Stato membro diverso da quello dove vi è la sede principale. Il Considerando 22 del GDPR conferma infatti che qualsiasi trattamento dati effettuato da una succursale o sede secondaria stabilita nel territorio dell'Unione europea deve essere sottoposto alle previsioni normative del Regolamento (UE) 2016/679, indipendentemente dal fatto che la gestione delle informazioni sia poi condotta effettivamente all'esterno dei confini europei.

Si avverte la volontà del legislatore UE di proporre una normativa forte e che possa funzionare da modello globale per la tutela della privacy e dell'autonomia informativa, salvaguardando così la sicurezza dei propri cittadini anche al di fuori del territorio dell'Unione europea[493].

[493] M.G.STANZIONE, *Genesi e ambito di applicazione,* Cap.II, in (a cura di) S.SICA, V.D'ANTONIO, G.M.RICCIO, *cit.*, pp.31.

5.4. Privacy by design e Privacy by default: il Regolamento (UE) 2016/679 introduce due nuovi approcci alla protezione dei dati personali

Il Regolamento (UE) 2016/679 adotta un approccio volto a responsabilizzare (*accountability*) il titolare del trattamento dati e a far sì che questo soggetto adotti pratiche e accorgimenti che tengano conto dei diritti e delle libertà delle persone interessate dalla raccolta e dalla gestione delle informazioni. Seguendo tale ottica, l'art.25 del GDPR introduce il concetto di *privacy by design* per il quale è necessario garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.

Secondo tale principio[494], qualsiasi processo di raccolta e gestione delle informazioni deve essere ideato e progettato tenendo primariamente conto dei profili di riservatezza e di protezione dei dati personali dei soggetti coinvolti. Le misure tecniche e organizzative sono quindi prefissate dal titolare del trattamento e ne caratterizzano lo svolgimento sin dalle sue fasi iniziali.

Si assiste a un radicale cambio di prospettiva[495] rispetto allo schema precedente secondo il quale la tecnologia precedeva logicamente e cronologicamente la normativa: è infatti quanto previsto dall'art.25 GDPR a dettare gli schemi che devono essere seguiti nella progettazione delle innovazioni tecnologiche.

Il principio della *privacy by default*, introdotto dal medesimo articolo, opera invece in un secondo momento, imponendo al titolare di predisporre misure specifiche per garantire un idoneo trattamento dei dati raccolti secondo le finalità e gli scopi prefissati e rispettando altresì il principio di necessità e proporzionalità della *data protection.*

5.5. I diritti garantiti all'interessato dal Regolamento (UE) 2016/679

Il Regolamento (UE) 2016/679 dedica un intero Capo, il terzo, ai diritti dell'interessato dal trattamento dei propri dati personali, a differenza di quanto accadeva

---

[494] Per un esame teorico approfondito della *privacy by design* si fa riferimento ad A.CAVOUKIAN, *Privacy by design. The 7 foundational principles*, https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (consultato il 20 agosto 2019).

[495] R.PANETTA, *Privacy by design e GDPR: un'etica per l'intelligenza artificiale,* in *Agenda Digitale*, 11 ottobre 2018, https://www.agendadigitale.eu/sicurezza/privacy/privacy-by-design-e-gdpr-unetica-per-lintelligenza-artificiale/ (consultato il 20 agosto 2019).

nella previgente Direttiva che non prevedeva un unico paragrafo organico per l'elencazione e la disciplina di suddetti diritti. L'intenzione del legislatore europeo è quella di fornire a tal proposito una regolamentazione omogenea e uniforme, distinguendola dalla restante normativa tecnica e di dettaglio.

L'influenza causata dalle innovazioni tecnologiche sul GDPR non passa certo inosservata; alcuni dei diritti garantiti dal nuovo Regolamento rispondono infatti a precise esigenze avvertite dalla società moderna al mutare delle condizioni socio-economiche e all'avvento delle nuove tecnologie digitali di comunicazioni che, se non adeguatamente regolamentate, possono avere un impatto devastante sulla privacy e sull'autonomia informativa dei cittadini europei.

5.5.1. L'interconnessione globale e il diritto alla portabilità dei dati

Un esempio di come il Regolamento (UE) 2016/679 ha recepito le istanze determinate dal nuovo contesto tecnologico è dato dal cd. diritto alla portabilità dei dati. Lo spazio cibernetico ha ormai raggiunto una dimensione globale e numerosi sono gli attori che popolano questa dimensione virtuale; gli utenti possono infatti rivolgersi a diversi fornitori di servizi che utilizzano però strutture informatiche non compatibili tra loro, con conseguenti problemi tecnici di compatibilità.

Il nuovo Regolamento prevede, all'art.20, il cd. diritto alla portabilità dei dati, che consente al soggetto interessato di richiedere le proprie informazioni personali fornite al responsabile del trattamento dati in un formato strutturato, di uso comune e leggibile attraverso mezzi automatici, senza che il predetto responsabile possa ostacolare o rifiutarsi di soddisfare tale richiesta. La *ratio legis* è di concedere la possibilità all'interessato di valutare quali sono le informazioni condivise e di riappropriarsene. Una simile facoltà dovrebbe permettere una più agevole circolazione dei dati personali, a favore dei consumatori che potranno rientrare in possesso delle informazioni cedute a un gestore di servizi per l'ottenimento di una prestazione al fine di rivolgersi a un altro operatore del settore[496].

[496] L.VALLE, L.GRECO, *Transnazionalità del trattamento dei dati personali e tutela degli interessati tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale,* in *Diritto dell'Informazione e dell'Informatica*, fasc.2, aprile 2017, pp.168 ss.

Il Regolamento sembra incentivare una sorta di "interoperabilità"[497] della lettura di tali dati, indipendentemente dall'attore incaricato, e porre dei requisiti minimi a cui i gestori del trattamento delle informazioni devono adeguarsi al fine di raggiungere l'obbiettivo della portabilità dei dati. Lo stesso regolamento, tuttavia, al considerando 68 dispone altresì – apparentemente contraddicendosi – che il diritto del soggetto a trasmettere e ricevere i propri dati personali *non* crea un'obbligazione per il responsabile del trattamento ad adottare specifici sistemi tecnici e informatici.

L'applicazione di quanto previsto dall'art. 20 del Regolamento è soggetta inoltre a determinati requisiti legali, poiché può essere richiesta esclusivamente per i dati personali per cui il soggetto ha acconsentito al trattamento. Il diritto alla portabilità non viene esteso ai dati che il gestore del trattamento ha tratto da altre fonti e che non provengono quindi dal diretto interessato. Si potrebbe perciò riscontrare una qualche contraddittorietà rispetto a quanto affermato dall'art. 15 (3) dello stesso Regolamento, che prevede il diritto per il soggetto interessato di richiedere una copia delle proprie informazioni trattate, senza però poterne domandare anche la portabilità. Al fine di ovviare a questa possibile discrasia, è stata proposta un'interpretazione del dettato normativo più ampia ed estensiva, includendo quindi anche dati generati da un fornitore di servizi attraverso processi quali l'utilizzo di algoritmi. Un'ulteriore eccezione all'applicazione del diritto alla portabilità si ha quando il trattamento dei dati personali è necessario al perseguimento di finalità di pubblico interesse o quando è portato avanti da un'autorità pubblica nell'esercizio delle sue funzioni.

5.5.2. L'evoluzione del diritto all'oblio e la sua disciplina all'interno del Regolamento (UE) 2016/679

Una delle innovazioni più rilevanti apportate dal Regolamento (UE) 2016/679 è stata senza dubbio la disciplina normativa del cd. diritto all'oblio. Con tale termine si vuole indicare una modalità di esercizio del proprio diritto all'identità personale, chiedendo di dimenticare (obliare) cosa si ritiene non sia più pertinente alla propria individualità[498].

[497] L.SCUDIERO, *Bringing your data everywhere: a legal reading of the right to portability*, in *European Data Protection Law Review*, n.1, 2017, pp.119-127.
[498] G.TROIANO , *Diritto all'oblio e privacy, cos'è e come esercitarlo:tutto quello che devi sapere*, in *Agenda Digitale,* 14 marzo 2018, https://www.agendadigitale.eu/sicurezza/il-diritto-alloblio/ (consultato il 21 agosto 2019).

Una prima formulazione del diritto all'oblio risaliva all'epoca *off-line*[499], quando il *cyberspace* non aveva ancora raggiunto gli attuali livelli di pervasività e diffusione; allora l'obbiettivo era quello di limitare la reiterazione di una particolare notizia che si riteneva avesse perso il proprio interesse pubblico con il passare del tempo e che non descrivesse perciò più l'attuale stato delle cose, limitandosi a diffondere un'immagine dei soggetti coinvolti non più attuale e quindi potenzialmente lesiva. Il diritto all'oblio vantato dal singolo individuo si poneva perciò in una potenziale antitesi con il diritto di cronaca e con il diritto degli altri consociati ad essere informati[500].

Nell'epoca della società digitale, dove ogni utente cibernetico è una potenziale fonte di diffusione di informazioni, risulta spesso assai complesso e farraginoso esercitare tale prerogativa. Il fattore tempo non gioca infatti lo stesso ruolo discriminante nell'ambito virtuale[501], non essendoci un'effettiva distinzione cronologica tra pubblicazione *on-line* della notizia e sua effettiva ripubblicazione. L'informazione rimane infatti disponibile sul *web* per ogni utente sin dal momento della sua prima condivisione. Il diritto all'oblio non si manifesta perciò nella richiesta di non procedere a una nuova reiterata diffusione della notizia, poiché questa rimane liberamente consultabile. L'informazione oggetto di questione deve essere invece aggiornata, in maniera tale che rispecchi la realtà attuale dei fatti e non risulti quindi potenzialmente lesiva; risulta quindi evidente lo stretto collegamento tra autonomia informativa e diritto all'identità personale.

Un'ulteriore evoluzione della concezione del diritto all'oblio si è avuto con la celebre sentenza *Google Spain*[502] con la quale la Corte di giustizia dell'Unione europea ha avuto l'occasione di proporre una formulazione di detto diritto che tenesse di conto il ruolo svolto dai motori di ricerca nell'attuale sistema di circolazione delle informazioni. Secondo i giudici della Corte spetta infatti a tali operatori intervenire direttamente per "ostacolare" la navigazione nei siti informatici che riportano la notizia che si vuole far cadere nell'oblio, operando una loro espunzione dai risultati di ricerca, chiamata "de-indicizzazione". Non si ottiene perciò una cancellazione dell'informazione controversa, bensì un suo "nascondimento" ottenendone una più difficile consultazione.

---

[499] V.D'ANTONIO, *Oltre la cancellazione dei dati personali: l'originaria concezione del diritto all'oblio off-line*, in (a cura di) S.SICA, V.D'ANTONIO, G.M.RICCIO, *cit.*, pp.203 ss.

[500] V.D'ANTONIO, *The right to tell people what they don't want to hear: i moderni confini del diritto di fare informazione*, in (a cura di) V.D'ANTONIO, S.VIGLIAR, *Studi di diritto della comunicazione. Persone, società e tecnologie dell'informazione*, Padova, 2009, pp.1 ss.

[501] G.FINOCCHIARO , *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Diritto dell'Informazione e dell'Informatica,* 2014, pp.593.

[502] Corte di giustizia dell'Unione europea, sentenza del 13 maggio 2014, *Google Spain*, causa C-131/12, ECLI: ECLI:EU:C:2014:317.

L'art.17 del Regolamento (UE) 2016/679 ha certamente risentito dell'influenza della pronuncia *Google Spain* nel definire e regolamentare il diritto all'oblio. Secondo quanto stabilito dal GDPR, l'interessato può richiedere la cancellazione delle informazioni che lo riguardano al titolare, e questo deve procedere senza ingiustificato ritardo se sussistono una serie di requisiti, tra cui il rispetto dei principi di legittimità, proporzionalità, necessità del trattamento dati.

5.5.3. Il diritto all'accesso ai propri dati personali nel Regolamento (UE) 2016/679 come prerogativa per l'esercizio dell'autonomia informativa

Il diritto all'accesso consiste nella possibilità per l'interessato di "accedere" ai propri dati personali e di essere reso edotto da parte del responsabile del trattamento delle modalità attraverso le quali suddetti dati vengono gestiti e per quali finalità. Il raggiungimento di una piena autonomia informativa, ossia dell'effettiva consapevolezza da parte dell'interessato di quali informazioni che lo riguardano sono state condivise non può infatti prescindere da una piena collaborazione tra quest'ultimo e il titolare del trattamento.

Il diritto all'accesso permette alla persona di avere un pieno controllo della propria identità elettronica[503] e di poter esercitare tutta la serie di diritti fino ad ora esposta, comprensiva del diritto all'oblio e alla portabilità dei dati.

L'art.15 del Regolamento (UE) 2016/679, tenendo presente quanto detto finora, riconosce all'interessato il diritto di sapere dal titolare se esiste un trattamento dati che lo vede coinvolto; nel caso positivo ha altresì il diritto di essere informato in merito alle finalità di suddetto trattamento, ai soggetti con i quali le informazioni che lo riguardano vengono condivise e ai tempi di conservazione di tali dati.

[503] F.M.DONNINI, *op.cit.*

5.6. Il trasferimento dati fuori dai confini europei sotto l'egida del Regolamento (UE) 2016/679

La diffusione globale della rete internet ha reso ormai possibile il trasferimento di dati e informazioni tra i vari Paesi, senza che confini territoriali e diverse disposizioni normative nazionali possano essere di ostacolo. La diffusione e la commercializzazione di dati sono ormai elementi fondamentali dell'economia odierna.

Secondo la disciplina prevista dall'art. 25 della direttiva 95/46, trasferimenti transfrontalieri di informazioni sensibili potevano essere autorizzati solo verso Paesi terzi che, su giudizio della Commissione europea, presentassero un livello di tutela della riservatezza adeguato rispetto agli standard europei. La normativa prevedeva delle deroghe, elencate tassativamente, al giudizio preventivo della Commissione, che poteva essere ovviato qualora il trasferimento dei dati è necessario per finalità quali la chiusura di un contratto, la salvaguardia di un interesse pubblico o di un interesse fondamentale della persona.

Il nuovo GDPR dedica diversi articoli, dal 44 al 50, alla regolazione dei trasferimenti dei dati personali oltre i confini nazionali; il testo del regolamento riconosce il diritto all'identità personale e alla salvaguardia della riservatezza delle informazioni sensibili trattate oltre frontiera, riprendendo e specificando inoltre, all'art. 45, il concetto di "adeguatezza" che caratterizzava il giudizio della Commissione ai sensi della previgente disciplina. Lo standard di protezione richiesto al Paese terzo non deve essere identico a quello previsto dalla normativa europea, ma deve essere a questo equivalente, applicandolo inoltre alla luce di quanto previsto dalla Carta dei diritti fondamentali dell'Unione europea[504]. Il Regolamento specifica che la Commissione, nel suo giudizio di adeguatezza, è tenuta a verificare ulteriori criteri politici e sociali che dovrebbero evidenziare l'attenzione del Paese terzo alla corretta tutela dell'identità personale dei soggetti coinvolti, oltre quelli prettamente tecnico-giuridici. Il GDPR prevede inoltre un riesame su base quadriennale delle conclusioni formulate dalla Commissione nel suo giudizio, al fine di valutare eventuali evoluzioni da parte del Paese esaminato. L'art.49 elenca le deroghe, riprese perlopiù dalla previgente direttiva, che permettono il trasferimento transfrontaliero dei dati anche in mancanza dei requisiti summenzionati; un'importante aggiunta che viene fatta è relativa al perseguimento dell'interesse del

[504] C.KUNER, *Reality and illusion in EU data transfer Regulation post Schrems,* in *German Law Journal,* n.18, 2017, pp.881-914.

titolare del trattamento, qualora questo abbia valutato tutte le circostanze del caso e abbia fornito adeguate garanzie di tutela dell'identità personale del soggetto interessato.

6. Il Regolamento (UE) 2016/679 come nuovo standard globale in termini di tutela dell'autonomia informativa e di data protection

Come si è appena esaminato, l'odierna società digitale è caratterizzata da continui trasferimenti di informazioni attraverso il *web* che non risentono di confini politici o giuridici. Numerosi agenti economici trattano quotidianamente i dati personali di soggetti diffusi in ogni angolo del pianeta, dovendo quindi confrontarsi continuamente con un vero e proprio "rompicapo" normativo che deve tenere conto delle diverse legislazioni nazionali che vengono coinvolte in dette operazioni.

Considerata la pervasività globale dello spazio cibernetico, la tutela fornita dagli ordinamenti statali ai dati personali dei propri cittadini rischia di limitare la propria applicazione ai confini nazionali, diventando sostanzialmente inefficace.

Il Regolamento (UE) 2016/679 si propone perciò l'ambizioso obbiettivo di affermarsi come uno standard normativo riconosciuto a livello internazionale e non solamente europeo, in maniera tale da garantire il medesimo livello di protezione anche al di fuori del territorio dell'Unione europea. Il cd. criterio dello stabilimento, sancito dall'art.3 (1) del GDPR prevede l'applicazione del Regolamento ai trattamenti dati condotti dal titolare nell'ambito delle attività di uno stabilimento con sede europea, indipendentemente dal fatto che detto trattamento sia effettivamente condotto all'interno dei confini europei. Non ha quindi importanza il luogo geografico in cui sono concretamente portate avanti le azioni di raccolta e gestione delle informazioni, a patto che tra tali condotte e le attività dello stabilimento europeo ci sia un riconosciuto collegamento funzionale. La formulazione dell'art.3 (1) risente indubbiamente dell'influenza della sentenza *Google Spain* precedentemente esaminata, dove la Corte di giustizia dell'Unione europea aveva trovato tale collegamento tra la raccolta dati condotta da *Google* e le attività della sua succursale spagnola.

Rappresenta una sostanziale novità nella normativa in materia di *data protection* il cd. *targeting criterion*[505] , affermato dall'art.3 (2), secondo il quale il GDPR trova

[505] Guidelines 3/2018 on the territorial scope of the GDPR (article 3) – Version for public consultation, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf (consultato il 22 agosto 2019).

applicazione nei confronti di trattamenti dati condotti da un titolare o un responsabile esterno al territorio europeo per finalità quali l'offerta di beni o servizi a persone che si trovano all'interno dei confini europei o il monitoraggio del loro comportamento finché questo si esplica all'interno dell'Unione.

Viene meno qualsiasi riferimento alla nazionalità dei soggetti coinvolti, poiché rileva esclusivamente la loro presenza sul territorio europeo al momento della raccolta e della gestione delle informazioni.

Occorre però ricordare un recente aggiornamento giurisprudenziale in merito all'effettiva portata applicativa del GDPR, con particolare attenzione al diritto all'oblio. La Corte di giustizia, con la pronuncia CNIL[506], ha chiarito la valenza territoriale del diritto alla deindicizzazione, ossia la richiesta avanzata dall'interessato nei confronti del gestore di un motore di ricerca di cancellare uno o più risultati di navigazione ottenuti digitando il proprio nome. I giudici hanno specificato che la portata della deindicizzazione deve ritenersi coincidente con il territorio dell'Unione europea, poiché il GDPR non dà alcun potere alle autorità di garanzia di adottare alcuna decisione che dispieghi i propri effetti anche al di fuori del territorio europeo. Viene lasciato ad eventuali misure normative adottate dai singoli Stati membri il compito di determinare possibili accorgimenti per ottenere una deindicizzazione a livello globale. La decisione della Corte di giustizia nel caso in esame sembra mettere in discussione quanto precedentemente affermato nella famosa sentenza *Google Spain*, dove veniva riconosciuto un diritto all'oblio senza distinzioni di confini od ordinamenti normativi. La pronuncia CNIL sembra non tenere conto della natura decentralizzata e diffusa della rete Internet; non vi è ragione apparente per cui la rimozione di determinati contenuti, avvenuta su richiesta dell'interessato, debba essere limitata a una sola parte della rete e non avere effetti sulla totalità del *web*. In tale maniera la persona non ha effettivamente disponibilità delle informazioni che la riguardano, venendo quindi meno l'essenza stessa del diritto alla protezione dei dati personali[507].

Alla luce dei criteri ora esposti, si comprende la volontà del legislatore europeo di garantire un ambito applicativo globale per il GDPR. Pressoché ogni minimo collegamento con l'Unione europea, che sia attraverso la localizzazione di uno

[506] Corte di giustizia dell'Unione europea, sentenza del 24 settembre 2019, causa C-507/17, *CNIL*, ECLI:EU:C:2019:772.
[507] F.B.ROMANO, *La Corte di giustizia resetta il diritto all'oblio,* in *federalismi.it*, 5 febbraio 2020, pp.1-17.

stabilimento del titolare del trattamento dati o per la posizione geografica dei soggetti coinvolti, comporta l'inesorabile operatività del Regolamento (UE) 2016/679.

Una simile realtà dei fatti pone le industrie e aziende coinvolte di fronte a un bivio: optare per il medesimo livello di protezione garantito dal GDPR anche per le operazioni condotte al di fuori dell'ambito di applicazione del Regolamento, assumendo così un'unica e sola *privacy policy*, o preferire invece un duplice standard di tutela, a seconda dei soggetti coinvolti?

Scegliere la prima opzione comporterebbe delle importanti conseguenze, *in primis* il sostanziale riconoscimento dei diritti garantiti dal GDPR anche a cittadini non europei.

L'approvazione e l'entrata in vigore del Regolamento (UE) 2016/679 riveste un'importanza cruciale anche per quanto riguarda il trasferimento transfrontaliero di dati al di fuori dei confini europei; come spiegato poc'anzi, la Commissione può autorizzare il flusso di informazioni solo verso Paesi che rispettano standard adeguati in materia di *data protection*. Il GDPR rappresenta ad oggi tale livello di adeguatezza.

Questo comporta che il Regolamento 2016/679 può assumere una funzione di modello a cui aspirare per le successive legislazioni internazionali ed extra-europee; gli Stati esterni all'Unione sono spinti ad adottare misure normative in linea con il GDPR per permettere gli scambi di dati con il mercato europeo.

Alla luce di quanto esposto, si può concludere che il diritto all'autonomia informativa e alla *data protection* sta assumendo una dimensione sempre più globale con la tutela garantita dal GDPR.

Osservazioni conclusive

Questo studio ha voluto svolgere alcune riflessioni in merito alla natura dello spazio cibernetico e alle effettive possibilità di regolamentare tale nuovo ambiente, nella prospettiva di tutelare e salvaguardare i diritti fondamentali dei cibernauti.

Il primo capitolo ha avuto l'obbiettivo di studiare le caratteristiche del *cyberspace*, evidenziando inoltre come queste influissero sui tentativi normativi volti proprio a regolamentare la dimensione cibernetica che si sono succeduti nel corso degli anni. Il mondo virtuale ha infatti posto a dura prova i legislatori statali e sovranazionali, per non parlare di studiosi e accademici che si sono succeduti, con relativo successo, a formulare

diverse teorie riguardanti l'essenza dello spazio cibernetico e il ruolo che gli Stati devono avere in esso.

La teoria del *Cyberlibertarianism*, che trova il suo prodotto principale nella celebre *Declaration of the Independence of Cyberspace* di J.P.Barlow, è nata in un'epoca in cui l'accesso a Internet era limitato e disponibile solamente a un relativamente ristretto numero di esperti del settore informatico. Il *world wide web* non aveva ancora la connotazione di fenomeno comunicativo di massa che ha invece oggigiorno. In ragione di ciò, i primi cibernauti hanno ritenuto che lo spazio cibernetico potesse provvedere in autonomia alla propria regolamentazione; il ristretto numero di utenti sembrava non necessitare di un intervento statale sul piano regolamentare e legislative.

Considerato inoltre che tali soggetti erano in possesso di un elevato grado di competenza tecnica e informatica che permetteva loro di operare in autonomia cambiamenti operativi ai sistemi digitali.

La diffusione a livello globale di Internet e il ruolo sempre più importante che la rete informatica ha acquisito nella vita quotidiana hanno portato alla luce i difetti della teoria del *Cyberlibertarianism*: lo spazio cibernetico è una creazione artificiale dell'essere umano, e come tale non ha alcun "istinto" all'autodisciplina.

Gli Stati, consapevoli della crescente importanza del *cyberspace* nella società e nell'economia, iniziavano inoltre a rivolgere le loro attenzioni al territorio virtuale, riflettendo sulle corrette modalità con le quali regolamentare le relazioni e gli accadimenti che si svolgevano in tale dimensione. La teoria del *Cyberpaternalism* ha legittimato l'intervento statale nel virtuale: lo spazio cibernetico non era più qualcosa di distante dalla realtà concreta e limitato all'utilizzo di pochi esperti informatici, ma una dimensione strettamente connessa al mondo fisico, a cui i legislatori nazionali potevano estendere la propria sfera di influenza.

Ben presto è risultato però chiaro che gli strumenti normativi tradizionalmente utilizzati non avevano lo stesso grado di efficacia quando erano calati nel contesto cibernetico; non era infatti possibile ritrarre la complessità e le innovazioni del mondo virtuale attraverso le categorie giuridiche ideate e impiegate nella realtà fisica concreta, a causa della complessità ontologica stessa del *cyberspace*. Si parla infatti di uno spazio che trascende qualsiasi localizzazione geografica e oltrepassa i confini delle singole nazioni; un'azione o un accadimento possono avere conseguenze globali. I concetti di sovranità e giurisdizione statale devono essere perciò ripensati alla luce di questa nuova realtà a dimensione sovranazionale.

Considerato ciò, il tentativo di normazione dello spazio cibernetico non può esaurirsi a un livello locale, dovendo giocoforza coinvolgere l'intera comunità internazionale. Un progetto legislativo di simile portata rischia però di rimanere un mero auspicio, a causa dei molteplici interessi socio-economici in gioco e delle diverse visioni politiche, spesso contrapposte, che animano i singoli Stati. I Paesi cd. occidentali, dove il *world wide web* ha visto la luce, si sono fatti promotori di una rete Internet liberamente accessibile ai singoli utenti, dove gli internauti possono comunicare ed esprimere le proprie opinioni senza dover temere alcuna censura, se non in limitati e ristretti casi specifici. Di diversa opinione sono le nazioni sotto la sfera di influenza della Russia e della Cina, dove l'intervento statale nella regolamentazione della circolazione delle informazioni è prassi comune e regolamentata.

Di fronte a un simile stallo, la volontà di legiferare in materia cibernetica rischia di scontrarsi contro una realtà politica non ancora pronta ad affrontare tale problema. Per poter trovare una base comune su cui dialogare e da cui partire per formulare una disciplina del *cyberspace*, può essere utile rifarsi alle precedenti esperienze regolamentatrici in territori caratterizzati da un certo grado di internazionalità: l'alto mare, lo spazio celeste e il continente antartico. Come si è visto durante il presente studio, queste realtà sono disciplinate attraverso l'utilizzo di trattati internazionali, dove tali spazi vengono preservati da mire espansionistiche statali per un utilizzo pacifico da parte dell'intera comunità internazionale.

Non bisogna però trascurare una grande differenza che intercorre tra i territori appena menzionati e lo spazio cibernetico: la presenza attiva di importanti soggetti privati (si pensi a tal proposito alle grandi compagnie come Google, Apple, Microsoft etc. etc.) che contribuiscono a trasformare in maniera costante la realtà informatica attraverso il loro operato. Proprio per la loro innegabile importanza nel contesto cibernetico, questi attori hanno un'importante voce in capitolo nella disciplina del *cyberspace* e devono essere perciò tenuti in considerazione da qualunque tentativo di normazione del mondo virtuale.

Data la molteplicità degli interessi in gioco, dei diversi orientamenti politici e dei numerosi ordinamenti giuridici coinvolti, attualmente il risultato di una regolamentazione uniforme e omnicomprensiva del contesto cibernetico e al di là da venire: si è preferito concentrare gli sforzi su determinati singoli aspetti, disciplinati di volta in volta attraverso specifici trattati internazionali.

In mancanza di una visione comune, la tutela dei diritti fondamentali può rappresentare una base condivisa su cui sviluppare in maniera graduale un tessuto normativo universalmente accettato per lo spazio cibernetico. Come saggiamente osservato dal prof.Giovanni Sartor, i diritti fondamentali possono rappresentare quell'unità normativa indissolubile e imprescindibile anche nel contesto virtuale. Gli internauti devono poter navigare sul *world wide web* in piena sicurezza, potendo legittimamente aspirare a che le proprie prerogative umane fondamentali vengano compiutamente rispettate, così come dovrebbe auspicabilmente già succedere nella realtà concreta.

Partendo da questo presupposto, lo studio si è sviluppato verso molteplici direzioni, andando ad analizzare i diritti fondamentali che si sono ritenuti più importanti nel contesto virtuale. Lo scopo è stato quello di valutare se sussistono elementi comuni e/o tratti distintivi in merito alle diverse previsioni normative già esistenti in merito alla tutela di tali diritti su cui iniziare eventualmente una riflessione che coinvolga poi l'intera realtà cibernetica.

Al fine di poter esprimere liberamente la propria personalità nel contesto virtuale e di usufruire del mezzo di comunicazione globale che è diventato il *world wide web*, la persona deve essere dotata degli strumenti necessari per poter accedervi: non si può parlare di diritti fondamentali nel *cyberspace* se non si è in grado di navigare nello spazio cibernetico.

Considerato ciò, il presente studio ha voluto riflettere sull'effettiva natura del diritto all'accesso a Internet: può essere considerato come un nuovo diritto fondamentale? Il dibattito volto a rispondere a questa domanda ha coinvolto accademici, politici, legislatori e tecnici informatici.

Coloro che hanno rifiutato di vedere nell'accesso a Internet un diritto imprescindibile dell'essere umano hanno sostenuto tale convinzione basandosi sul fatto che si tratta solamente di una tecnologia, ossia di un mezzo per poter esercitare le proprie prerogative e non di un diritto in *re ipsa*. Di diversa opinione sono coloro che hanno condannato l'"oblio digitale" a cui sono sottoposti gli individui che non hanno i mezzi per potersi connettere a Internet. Lo spazio cibernetico è infatti l'ambiente dove quotidianamente le persone esercitano i propri diritti, intrecciano relazioni di ogni tipo e si rivolgono alle istituzioni pubbliche.

Il diritto all'accesso a Internet non ha infatti solamente una dimensione negativa, consistente nel diritto del cittadino a non subire ingerenze di alcun tipo da parte dello

Stato e dei pubblici poteri nell'esercizio della sua libertà di connettersi al mondo virtuale, ma ha anche una valenza positiva. Si pensi a una pretesa del cittadino di vedersi forniti i mezzi per poter navigare nello spazio cibernetico: una pretesa non particolarmente differente da quello che accade con altri servizi come l'istruzione o la sanità.

Il costante progresso tecnologico fa sì che il mondo cibernetico sia in costante mutamento, rendendo assai complesso inquadrarlo in categorie giuridiche e normative stabili e durature. Non è perciò semplice individuare in cosa debba effettivamente consistere la pretesa, di cui si è appena accennato, dei cittadini nei confronti dei pubblici poteri per vedersi riconosciuto l'accesso a Internet. Si tratta di avere a disposizione dei *device* dotati di connessione *web*? Di ricevere un'adeguata educazione digitale? Bisogna poi riflettere su quale tipo di spazio cibernetico è al centro della discussione: si vuole ottenere una rete neutrale, ossia che non privilegi alcuni contenuti a discapito di altri?

Per poter rispondere in maniera adeguata a questi quesiti, occorre tenere in considerazione una serie di fattori. La dimensione cibernetica è caratterizzata dalla coesistenza di una molteplicità di soggetti, sia di origine pubblica che privata. Alcuni di loro, come le grandi compagnie di telecomunicazioni e gli operatori *over the top*, hanno una dimensione e un potere tale che contribuiscono in maniera fondamentale alla prassi cibernetica e a caratterizzarne gli elementi regolamentatori. Possiedono infatti la strumentazione necessaria ad accedere al mondo virtuale (cavi, *router*, *server* etc) dove immettono i propri contenuti (si pensi ad esempio ai siti di *social network* che aumentano i propri iscritti giorno dopo giorno).

Questa breve specificazione è utile per comprendere che la realizzazione pratica e concreta del diritto all'accesso a Internet passa necessariamente dalla stretta collaborazione tra lo Stato e gli attori privati principali della dimensione cibernetica; un'imposizione unilaterale di origine pubblica non avrebbe alcuna efficacia. Le norme sarebbero interpretate come non ricevibili, poiché non giustificate dalla effettiva situazione dei rapporti tra i vari attori presenti nel *cyberspace*. Le azioni delle TelCo, così come i comportamenti degli operatori *over the top*, proprio per le caratteristiche dei soggetti da cui provengono, sono infatti in grado di orientare la prassi virtuale, orientandone in maniera definita i rapporti di forza.

Alla luce di ciò, si auspica una collaborazione tra l'autorità pubblica e i soggetti privati per arrivare a capire come attuare concretamente un diritto all'accesso a Internet per ogni persona, tenendo conto anche del legittimo interesse economico portato avanti dagli operatori del settore.

In vista dei possibili investimenti necessari per potenziare le infrastrutture necessarie per implementare una connessione globale, occorre tenere presenti le condizioni economiche dei vari Stati. I patrimoni nazionali dei vari Paesi non permettono certamente i medesimi investimenti per ogni nazione, ma questo non dovrebbe andare a detrimento dei cittadini degli Stati meno abbienti.

Ulteriori elementi da tenere in considerazione per stabilire come garantire una connessione al *cyberspace* su scala globale sono le diversità sociali proprie di ogni Paese. Le peculiari strutture politiche di ogni Stato, così come i differenti *background* culturali, sono infatti dei fattori che rendono assai complesso formulare un diritto all'accesso a Internet replicabile su scala globale. D'altro canto, un diritto fondamentale deve essere ontologicamente applicabile a ogni essere umano in quanto tale; deve essere perciò dotato di un certo grado di astrazione e svincolato da ogni possibile particolarismo. Più specificatamente, considerata proprio la natura diffusa e decentralizzata di Internet, sarebbe contraddittorio vincolare l'accesso alla rete a requisiti vincolati all'effettivo luogo di connessione o alla nazionalità dell'utente.

Premesse queste considerazioni, si comprende che, allo stato attuale delle circostanze, è complesso formulare in termini universalmente efficaci, sia sotto il lato giuridico che socio-economico, un diritto all'accesso a Internet. Occorre perciò individuare un nucleo fondante attorno al quale poter raccogliere il consenso di tutti gli attori cibernetici non tanto per garantire effettivamente una connessione globale, ma piuttosto per assicurare a ogni persona la possibilità di connettersi alla rete informatica a condizioni accettabili.

Per fare ciò, è necessario innanzitutto potenziare drasticamente le infrastrutture informatiche di quei Paesi che ancora non si sono dotati delle tecnologie necessarie; gli investimenti economici pubblici sarebbero poi ripagati dal successivo aumento di produttività dovuta all'informatizzazione. Di pari passo deve avvenire una progressiva educazione digitale delle persone; ogni individuo deve essere messo in grado di capire come sfruttare al meglio per la propria crescita, sia personale che lavorativa, gli strumenti offerti dalla rete. Un ulteriore ostacolo per un diritto all'accesso a Internet su scala globale è dato, come si accennava precedentemente, dalle diversità tra Stati in termini culturali e politici; si pensi ai regimi dittatoriali che impediscono l'accesso al *web* o alla fruizione di determinati contenuti da parte dei propri cittadini. Finché resistono simili realtà, sarà impossibile avere un vero e proprio diritto fondamentale all'accesso a Internet. Il potere della rete sta però proprio nella sua natura diffusa e sovranazionale; l'utilizzo di

strumentazioni tecnologiche adeguate e la "creatività" degli utenti nell'utilizzare i mezzi disponibili per lanciare qualsiasi tipo di messaggio[508] dimostrano come il *cyberspace* possa essere ostacolato, ma non totalmente arginato.

Fino a che la dimensione cibernetica non sarà liberamente accessibile in ogni sua realtà a ogni persona su una scala globale, la discussione passa giocoforza a un livello regionale. A tal proposito, l'importanza dell'utilizzo di Internet nella società odierna viene certificata anche dalla normativa dell'Ue che classifica la connessione a Internet come "servizio sociale", intendendosi con tale termine un numero minimo di prestazioni che devono essere garantite da parte dello Stato ai propri cittadini a uno standard qualitativo prefissato.

L'accesso a Internet è un prerequisito fondamentale per l'effettivo utilizzo di una serie di diritti nella società digitale, *in primis* il diritto alla libera espressione.

Si tratta di un valore dalla forte dimensione antagonista: hanno bisogno di tutela le idee minoritarie e difformi dall'opinione pubblica dominante.

La diffusione globale di Internet ha radicalmente trasformato il tradizionale meccanismo di circolazione delle informazioni, influenzando quindi anche il legame che intercorre tra la libertà di parola e il diritto all'informazione.

Nell'epoca pre-cibernetica, il ruolo predominante era svolto dalle grandi compagnie editoriali che, attraverso giornali e telegiornali, diffondevano le notizie a lettori e spettatori che erano relegati al ruolo di meri fruitori passivi: la circolazione delle informazioni avveniva quindi secondo un flusso verticale.

Questa situazione è mutata con l'avvento di Internet: ogni persona in possesso di un *device* connesso allo spazio cibernetico può diffondere su scala globale le proprie idee, senza aver bisogno di alcun filtro o intermediario. Una simile realtà ha indubbi lati positivi: qualsiasi utente cibernetico ha la possibilità di contribuire alla formazione della coscienza politica della comunità, avendo inoltre a disposizione un patrimonio pressoché inesauribile di informazioni.

Questa abbondanza di dati e notizie nasconde però delle insidie da non sottovalutare: fenomeni come le *fake news*, informazioni fasulle create artificiosamente con l'intento di inquinare il *public discourse* e orientare le scelte politiche ed elettorali

[508] Recentemente una ragazza ha utilizzato il *social network* TikTok per condividere un video in cui illustrava come truccarsi: nel bel mezzo del filmato, ha segnalato la situazione dei campi di concentramento cinesi contro la minoranza musulmana, https://www.open.online/2019/11/27/su-tiktok-finge-un-tutorial-sul-makeup-per-parlare-dei-lager-cinesi-beffa-alla-censura-di-pechino-video/ (consultato il 12 aprile 2020).

della collettività in una determinata direzione piuttosto che in un'altra, devono essere affrontati con la dovuta accortezza normativa.

Un ruolo importante nell'epoca digitale viene svolto dalle piattaforme di *social media*, come Facebook o Twitter: pur non essendo classificabili come produttrici di informazioni, su tali siti si possono trovare contenuti di ogni tipo. Viene perciò a mancare il lavoro di valutazione dell'attendibilità delle notizie che veniva precedentemente svolto dai giornalisti e dagli altri intermediari del mercato dell'informazione.

Le importanti novità tecnologiche e sociali che hanno caratterizzato tale mercato negli ultimi anni hanno messo a dura prova le tradizionali categorie giuridiche utilizzate per definire e tutelare il diritto alla libera espressione. Il mondo digitale ha svelato nuove sfide e nuovi pericoli che meritano attenta considerazione dai legislatori nazionali e internazionali.

Elemento imprescindibile per poter esercitare una vera ed effettiva libertà di parola è il non dover temere alcuna ritorsione per le opinioni espresse; questo è possibile solo se viene rispettato anche il diritto alla privacy e alla riservatezza.

Non bisogna considerare la privacy come un valore statico e immutabile, poiché ha subito notevoli variazioni nel corso degli anni, andando a rispondere alle esigenze di mutate circostanze sociali e geografiche. Dal celebre scritto di Warren e Brandeis, dove si invocava il diritto ad essere lasciati soli, figlio di un'epoca dominata dalla borghesia e dove la proprietà privata era un valore fondamentale, si è arrivati al principio dell'autonomia informativa. Nell'epoca della connessione globale, non sussistono più spazi riservati al singolo individuo; ogni *device* collegato a Internet condivide costantemente dati personali in ogni angolo del globo. Questo fa nascere l'esigenza per ogni individuo di essere costantemente aggiornato e consapevole su quali informazioni sta condividendo e per quali finalità.

L'Unione europea ha risposto a tale necessità con il Regolamento 2016/679; il Regolamento Generale sulla Protezione dei Dati aspira a fornire un'adeguata tutela dei dati personali nell'epoca digitale.

Al termine di queste riflessioni sullo stato attuale del mondo cibernetico, è possibile formulare alcune osservazioni conclusive in merito alla tutela dei diritti fondamentali nel contesto virtuale.

In primis, risulta evidente la necessarietà di un approccio uniforme e omnicomprensivo da parte dei legislatori nazionali e internazionali. Il diritto alla privacy è indissolubilmente legato alla libera espressione e viceversa, così come risulta

fondamentale l'accesso a Internet per poter esercitare i propri diritti nell'epoca digitale. Gli utenti cibernetici che non possono usufruire di un'effettiva autonomia informativa non sono altresì liberi di esprimere la propria opinione senza temere rappresaglie o censure.

Un ulteriore risultato è che non si può parlare dei diritti qui considerati in termini assoluti, dato che sono parimenti meritevoli di tutela e devono coesistere nell'unica dimensione cibernetica. Spetta quindi ai legislatori, da un punto di vista astratto e generale, e ai giudici, da una prospettiva invece concreta e particolare, trovare un efficace punto di equilibrio tra le diverse istanze in gioco. Questo non è sempre facile a causa del continuo mutamento socio-economico e tecnologico della dimensione cibernetica, che cambia rapidamente e propone nuove esperienze di "navigazione virtuale" ai propri utenti. Le previsioni normative in materia devono quindi presentare un certo gradi di flessibilità e astrattezza per potersi adeguare alle diverse circostanze del caso concreto e non venir meno alla loro funzione di tutela dei diritti fondamentali rilevanti nel contesto cibernetico.

Un esempio di questo difficile bilanciamento viene fornito dalla famosa sentenza *Google Spain* della Corte di giustizia dell'Unione europea dove i giudici hanno sottolineato che la libertà di espressione non può andare a prevaricare sulla riservatezza del singolo individuo. I criteri utilizzati dalle Corti per dirimere tali controversie sono diversi e devono essere giustificati dal caso concreto; ad esempio, si valuta se il contenuto che potrebbe ledere la privacy di un soggetto ha una valenza pubblica e quindi merita di essere diffuso o ha altrimenti esaurito la sua funzione giornalistica.

Considerato ciò, una tutela "a compartimenti stagni" dei singoli diritti fondamentali, qui considerati in ambito cibernetico, rischia di rivelarsi inefficace: si auspica perciò un approccio di insieme. Tale sforzo unitario deve tenere conto delle caratteristiche ontologiche del *cyberspace*: come si è visto, si tratta di un ambiente che non tollera confini di alcun tipo, siano essi geografici o giuridici. Un utente informatico condivide i propri dati personali su scala globale, così come può diffondere le proprie idee e opinioni in ogni angolo del pianeta in maniera facile e veloce. Non è pensabile di disciplinare una realtà così complessa come lo spazio cibernetico su base nazionale; previsioni nazionali difformi e contradditorie tra loro porterebbero a una tutela inefficace dei diritti fondamentali qui considerati.

Questa speranza si scontra però con l'attuale frammentazione politica e giuridica che riguarda la visione dei vari Stati verso la dimensione cibernetica. I diversi

orientamenti ideologici espressi dai singoli Paesi e i differenti interessi in gioco impediscono allo stato attuale delle cose la formulazione di una "Carta dei Diritti Fondamentali dello spazio cibernetico", sulla falsariga della Dichiarazione Universale dei Diritti Umani che vide la luce nell'ormai lontano 1948.

Un simile documento sarebbe però auspicabile sotto diversi punti di vista; *in primis*, qualora venisse emanato nell'ambito delle Nazioni Unite, darebbe un forte segnale politico di un'unità di intenti in campo cibernetico, al di là dei singoli particolarismi e retaggi nazionali. Alla stregua di quanto avvenuto per la Dichiarazione Universale, una Carta del *cyberspace* potrebbe poi funzionare da bussola per orientare le future legislazioni in materia, sia a livello nazionale che regionale. Indicherebbe poi la prassi a cui dovrebbero attenersi gli attori del mondo virtuale, anche e soprattutto quelli di origine privata come le TelCo e gli *over the top*. Per quanto riguarda la concreta formulazione dei vari articoli di questa ipotetica Carta cibernetica, questo lavoro ha dimostrato che esiste già un copioso materiale normativo e giurisprudenziale in materia di tutela dei diritti fondamentali in ambito virtuale. Si presenta però come un mosaico frammentato, privo di una direttrice comune, causando così una tutela difforme e non omogenea dei diritti considerati. La Carta del *cyberspace* servirebbe per l'appunto a fornire le "linee guida" attorno alle quali salvaguardare la sicurezza e la salute di ogni utente virtuale.

Purtroppo si tratta di un risultato non ipotizzabile nel breve periodo, quindi occorre riporre le speranze sull'azione dei principali attori nel contesto cibernetico e in particolar modo l'Unione europea. Considerata la sua importanza economica, tecnologica e politica, può infatti segnare il passo da seguire per la tutela dei diritti fondamentali in ambito cibernetico.

Deve essere accolta con particolare favore l'attuale diffusione a livello extra europeo del Regolamento 2016/679, che si sta affermando sempre più come standard normativo globale. Proprio a causa di una società digitale senza più confini di sorta, un attore importante a livello politico ed economico come l'Unione europea può segnare il passo nel proporre sistemi di tutela sempre più avanzati, non solo per quanto riguarda il diritto alla privacy, ma anche per il diritto alla libera espressione.

In mancanza di una normativa uniforme a livello internazionale, l'utilizzo di strumenti internazional-privatistici può essere un valido espediente per risolvere eventuali controversie e per garantire una tutela uniforme per i diritti degli utenti cibernetici; come detto poc'anzi, aziende e compagnie extra europee stanno adottando *privacy policies* in

linea con quanto previsto dal Regolamento 2016/679. L'individuazione, attraverso elaborazione giurisprudenziale, del concetto di "sede principale degli interessi", aiuta una tutela della dignità della persona contro abusi della libertà di espressione nel contesto cibernetico.

Lo studio dei diritti fondamentali nel *cyberspace* ha fornito importanti indicazioni per comprendere come può essere disciplinato l'intero mondo virtuale, o perlomeno quali direttive dovrebbero essere seguite in questo sforzo normativo. Un ruolo importante dovrà essere svolto dall'Unione europea quale attore principale nel campo cibernetico, sia a livello politico che normativo, al fine di trovare un'unità di intenti con gli altri protagonisti del mondo virtuale, sia pubblici che privati, con cui costruire una disciplina del *cyberspace*, proprio a partire dai diritti fondamentali quali unità basilari e imprescindibili.

Riferimenti bibliografici

Cap.1
Un nuovo territorio virtuale e la sua struttura di governo: la gestione del ciberspazio e la tutela dei diritti fondamentali

- BAIRD Z., *Governing the Internet: Engaging governments, businesses, no profits,* in *Foreign Affairs*, novembre/dicembre 2002, pp.15 ss.

- BELLI L., DE FILIPPI P., *Net neutrality compendium; human rights, free competion and the future of internet,* Cham, 2016.

- BENKLER Y., *From consumers to users, shifting the deeper structures of regulation toward sustainable commons and user access*, in *Federal Communications Law Journal*, n.52, 2000, pp.561-562.

- BIEGEL S., *Beyond our control,* Cambridge, 2001.

- BOOTBY W.H., *Methods and means of cyber warfare*, in *International Law Studies,* n.89, 2013, pp.387 ss.

- BURK D.L., *Trademarks along the Infobahn: a first look at the emerging law of Cybermarks,* in *University of Richmond Journal of Law and Technology*, 1, 1995, pp.12-14.

- CARBONE S.M., *I soggetti e gli attori nella comunità internazionale*, in (a cura di) CARBONE S.M. ET AL., *Istituzioni di Diritto Internazionale*, Torino, 2016, pp.1-47.

- CASSESE A., *Diritto internazionale*, Bologna, 2013.

- DEMCHAK C.C., DOMBROSKI P., *Rise of a cybered Westphalian age*, in *Strategic Studies Quarterly*, primavera 2011, pp. 32 e ss.

- DICKIE J., *Consumers and producers in EU E-Commerce Law*, Oxford, 2005.

- DODGE M., KITCHIN R., *Atlas of cyberspace*, New York, 2002.

- DREZNER D., *The global governance of the internet: bringing the State back in*, in *Political Science Quarterly*, n.119, 2004, pp 477 e ss.

- EICHENSER K., *The cyber-law of nations*, in *Georgetown Law Journal*, n.107, 2015, pp.317-380.

- FRANZESE P.W., *Sovereignity in cyberspace; can it exist?*, in *Air Force Law Review*, n.1, 2009, pp.17 ss.

- FROOMKIN M., *The internet as a source of regulatory arbitrage*, in (a cura di) KAHIN B., NESSON C., *Borders in cyberspace*, Cambridge, 1996.

- GARRASCOSA GONZALÈZ J., *The Internet – Privacy and rights relating to personality*, Londra, 2015.

- GILES K., *Prospects for the rule of cyberspace*, Carlisle PA, 2017.

- GOLDSMITH J., *How cyber changes the law of war*, in *European Journal of Legal Studies*, n.24, 2013, pp.129 e ss.

- GOLDSMITH J., WU T., *Who controls the internet: illusions of a borderless world*, Oxford, 2006.

- HARDIN G., *The tragedy of commons*, in *Science*, n.162, 1968, pp 1243 ss.

- JOHNSON D.R., POST D., *Law and borders-The rise of law in cyberspace*, in *Stanford Law Review*, n.48, 1996, pp.1367-1378.

- KANUCK S., *Sovereign discourse on cyber conflict under International Law*, in *Texas Law Review*, n.88, 2013, pp.1595-1599.

- KING J., GRINTER R.E., PICKERING J.M., *The rise and fall of Netville: The saga of a cyberspace construction Boomtown in the great divide*, in (a cura di) KIESLER S., *Culture of the internet*, 1997, Londra.

- KOH H.H., *International Law in cyberspace, Remarks as prepared for the delivery to the USCYBERCOM Inter-Agency Legal Conference* (18 settembre 2012), in *Harvard International Law Journal Online*, n.54, pp.1-8.

- LESSIG L., *Code 2.0*, New York, 2006.

- LESSIG L., *The Architecture of Innovation, Inaugural Meredith and Kip Frey Lecture in Intellectual Property at Duke University School of Law*, in *Duke Law Journal*, 2002, pp.1783-1786.

- MANADIAKI K., *Eu competition law, regulation and the internet; the case of net neutrality*, Alphen aan den Rijn, 2015.

- MARSDEN C.T., *Network neutrality: from policy to law to regulation*, Manchester, 2017.

- MIHR A., *Cyber justice. Human rights and good governance for the internet*, Berlino, 2017.

- MILLARD C., *Cyberspace and the no regulation fallacy*, in *Global Telecoms Business Yearbook 1995*, pp.17 ss.

- MIULLER M., MATHIASON J., MCKNIGHT L.W., *Making Sense of 'Internet Governance': Defining Principles and Norms in a Policy Context*, Syracuse, 2004.

- MURRAY A., *Information technology law: the law and the society*, Oxford, 2010.

- NUNIZATO D., *Virtual freedom: net neutrality and free spech in the internet age*, Stanford, 2009.

- NYE JR J.S.., *Nuclear lessons for cyber security*, in *Strategic Studies Quarterly*, inverno 2011, pp.20 e ss.

- PARRISH A., *The effects test: extraterritoriality's fifth business*, in *Vanderbilt Law Review*, n.61, 2008, pp.1455 ss.

- POST D.G., *Governing cyberspace*, in *Wayne Law Review*, 43, 1996, pp.155-171.

- REED C., *Making laws for cyberspace*, Oxford, 2012.

- REIDENBERG J., *Lex informatica: the formulation of information policy rules through technology*, in *Texas Law Review*, n.76, 1998, pp.553 ss.

- SARTOR G., *Human rights in the information society: utopias, dystopias and human values*, in (a cura di) DE AZEVEDO CUNHA M.V., DE ANDRADE N.N.G., LIXINSKI L., FETEIRA L.T., *New Technologies and Human Rights. Challenges to Regulation*, Burlington, 2013.

- SAVIN A., *Eu internet law*, Cheltenham, 2012.

- STROVEL A., *Net neutrality in Europe*, Bruxelles, 2013.

- TREVES T., *Diritto internazionale. Problemi fondamentali*, Milano, 2013.

- WAXMAN M.C., *Cyber-attacks and the use of force: back to the future of article 2(4)*, in *Yale Law Journal*, n. 36, 2011,pp.431-36.

- WIENER N., *La cibernetica: controllo e comunicazione nell'animale e nella macchina*, Cambridge, 1948.

- ZICCARDI P., voce *Consuetudine (dir.intern.)*, in *Enciclopedia del diritto*, vol. IX, Milano, 1961, pp.486.

Cap.2

Il diritto di accesso a Internet è un nuovo diritto fondamentale? La connessione al ciberspazio tra libera espressione e intervento statale

- AKANDJI-KOMBE J.F., *Positive obligations under the European Convention on Human Rights. A guide to the implementation of the European Convention on Human Rights*, in *Human Rights Handbook*, n.7, 2007, pp.5 ss.

- ALU A., *Il diritto di accesso ad Internet nell'ordinamento europeo*, in (a cura di) ALLEGRI M.R., D'IPPOLITO G., *Accesso a Internet e neutralità della rete fra principi costituzionali e regole europee*, Roma, 2017, pp.93-109.

- ALLEGRI M.R., *Riflessioni e ipotesi sulla costituzionalizzazione del diritto di accesso a Internet (o al ciberspazio?)*, in *Rivista dell'Associazione Italiana dei Costituzionalisti*, n.1/2016, 29 febbraio 2016, pp.1-31.

- ANANASSO A., ANANASSO F., *La neutralità della rete. Problematiche e aspetti regolamentari*, in (a cura di) ALLEGRI M.R., D'IPPOLITO G., *Accesso a Internet e*

neutralità della rete fra principi costituzionali e regole europee, Roma, 2017, pp.109-127.

- ARISTOTELE, *La Politica,* in (a cura di) VIANO C.A., *Politica e Costituzione di Atene di Aristotele*, Torino, 1992.

- BENKLER Y., *The wealth of networks. How social production transforms markets and freedom*, Yale, 2006.

- BERMAN J., WITZNER D.J., *Technology and democracy,* in *Social Research*, n.64, 1997, pp.1313-1315.

- BERNERS LEE T., ALPIN H., *Internet access is a human right,* https://www.ibiblio.org/hhalpin/homepage/publications/def-timbl-halpin.pdf.

- BENTIVEGNA S., *Disuguaglianze digitali. Le nuove forme di esclusione nella società dell'informazione*, Roma, 2009.

- BING J., *Building cyberspace: a brief history of Internet*, in (a cura di) BYGRAVE L.A., BING J., *Internet governance. Infrastructure and institutions,* Oxford, 2009.

- BROWNSWORD R., GOODWIN M., *Law and the technologies of the twenty-first century*, Cambridge, 2012.

- N.BOBBIO, *L'età dei diritti,* 1990, Torino.

- CERF V., *Internet access is not a human right,* in *New York Times,* 4 gennaio 2012, https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html.

- CHRISTOFFERSEN J., *Fair balance: a study of proportionality, subsidarity and primarity in the European Convention of Human Rights,* Londra, 2009.

- COSTANZO P., *I nodi della regolamentazione*, in *Diritto dell'Informazione,* n.4, 1999.

- COSTANZO P., *Miti e realtà dell'accesso a Internet. Una prospettiva costituzionalistica*, in *Consulta OnLine,* 17 ottobre 2012, http://www.giurcost.org/studi/Costanzo15.pdf.

- D'IPPOLITO G., *L'accesso a Internet come diritto sociale. Ecco perché è necessario,* in *Agenda Digitale,* 29 marzo 2017,https://www.agendadigitale.eu/infrastrutture/occorre-una-prospettiva-umana-per-la-nuova-generazione-di-internet/.

- D'IPPOLITO G., *La proposta di un art.34-bis in Costituzione,* in (a cura di) ALLEGRI M.R., IPPOLITO G.D', *Accesso a Internet e neutralità della rete fra principi costituzionali e regole europee*, Roma, 2017, pp.65-93.

- D'IPPOLITO G., *Neutralità della rete e uguaglianza: dallo stato di natura al diritto,* in (a cura di) PASSAGLIA P., POLETTI D., *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa, 2016, pp.325-337.

- DE HERT P., KLOZA D., *Internet (access) as a new fundamental right. Inflating the current rights framework?,* in *European Journal of Law and Technology*, vol.3,n.3, 2012, pp.1-32.

- DELONG BAS N.J., *The new social media and the Arab Spring*, in *Islamic Studies Online*, Oxford, 2011, http://www.oxfordislamicstudies.com/Public/focus/essay0611_social_media.html.

- DE MINICO G., *Diritti, regole e Internet,* in *Costituzionalismo.it***,** 8 novembre 2011, http://www.costituzionalismo.it/articoli/393/.

- DE MINICO G., *Regulation, banda larga e servizio universale. Immobilismo o innovazione?,* in *Politica del Diritto,* n.4/2009, dicembre 2009, pp.531-566.

- DE SCHUTTER O., *International human rights law,* Cambridge, 2010.

- DE SOLA POOL I., *Technologies of freedom,* Boston, 1984.

- EASTERBROOK F.H., *Cyberspace and the law of the horse,* in *University of Chicago Legal Forum,* vol. 207, 1996, pp.3 e ss.

- FROSINI T.E., *Il diritto costituzionale di accesso a Internet,* in *Rivista Telematica Giuridica dell'Associazione Italiana dei Costituzionalisti,* n.1/2011, pp.1-17.

- FROSINI T.E., *Libertè, egalitè, Internet,* Napoli, 2015.

- GOLDSMITH J., WU T., *Who controls the Internet? Illusions of a borderless world*, Oxford, 2006.

- GREER S., *The European Convention on Human Rights. Achievements, problems and prospects*, Cambridge, 2006.

- HOLMAN J., MCGREGOR M., *The Internet as commons: the issue of access,* in *Communication Law and Policy,* vol.10, n.3, 2005, pp.267-289.

- JASMONTAITE L., DE HERT P., *Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment?*, in *Research Handbook on Human Rights and Digital Technology*, Bruxelles, 2017, pp.157-179.

- KARAT Z.F., *Human rights worldwide: a reference handbook*, Amsterdam, 2006.

- KATZ I., *Web freedom faces greatest threat ever, warns Google's Sergey Brin*, in *Guardian*, 15 aprile 2012, https://www.theguardian.com/technology/2012/apr/15/web-freedom-threat-google-brin.

- KERR O.S., *Cybercrime's scope: interpreting access and consent in computer misuse statutes',* in *New York University Law Review*, n.78, 2003, pp.1596.

- KUNER C., *An international legal framework for data protection: issues and prospects*, in *Computer law and Security Review*, vol.25(4), 2009, pp.307-317.

- LESSIG L., *The law of the horse:what cyberlaw might teach,* in *Harvard Law Review*, vol.113 (2), 1999, pp.10 e ss.

- MARCELLI F., *L'accesso a Internet come diritto fondamentale? Tendenze del diritto internazionale e realtà dei fatti,* in (a cura di) PIETRANGELO M., *Il diritto di accesso a Internet,* 2010, Napoli, pp.99-108.

- MARSOCCI P., *Lo spazio di Internet nel costituzionalismo,* in *Costituzionalismo.it,* n.2/2011, pp.1-16.

- MODUGNO V.F., *I "nuovi diritti" nella giurisprudenza costituzionale*, Torino, 1995.

- MOWRABAY A., *The development of positive obligations under the European Convention on Human Rights by the European Court of Human Rights*, Londra, 2004.

- MURRAY A., *A Bill of Rights for the Internet,* 2010, *http://theitlawyer.blogspot.com/2010/10/bill-of-rights-for-internet.html.*

- NANNIPIERI L., *Costituzione e nuove tecnologie,* https://www.gruppodipisa.it/images/seminariDottorandi/2013/LORENZO_NANNIPIERI_Costituzione_e_nuove_tecnologie.pdf.

- NICITA A., *La neutralità della rete tra prospettive regolatorie e dilemmi irrisolti*, in (a cura di) ALLEGRI M.R., D'IPPOLITO G., *Accesso a Internet e neutralità della rete fra principi costituzionali e regole europee*, Roma, 2017, pp.135-143.

- NICKEL J., *Making sense of Human Rights: Philosophical reflections on the Universal Declaration of Human Rights*, Los Angeles, 1987.

- ODELLO M., CAVANDOLI S., *Emerging areas of human rights in the 21st century*, Londra, 2011.

- OAKERSON R., *Analyzing the commons: a framework*, in (a cura di) BROMLEY D.W., *Making the commons work: theory, practice and policy*, New York, 1992.

- OROFINO M., *La declinazione della net neutrality nel Regolamento europeo 2015/2120. Un primo passo per garantire un'Internet aperta?*, in *Federalismi.it*, n.2/2016, pp.2-25.

- POWELL A., BRYNE A., DAILEY D., *The essential Internet: digital exclusion in low-income American communities*, in *Policy and Internet*, 2(2), 2010, pp.161-163.

- RIFKIN J., *L'era dell'accesso. La rivoluzione della New Economy*, Milano, 2000.

- RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004.

- ROZO SORDINI P.E., *La libertà di espressione nell'era digitale: disciplina internazionale e problematiche*, ISPI Working Paper n.52, Ottobre 2013, https://www.ispionline.it/sites/default/files/pubblicazioni/wp_52_2013.pdf.

- RUSSO S., SCIUTO A., *Habeas data e informatica*, Milano, 2011.

- SEGURA SERRANO A., *Internet regulation and the role of international law*, in *Max Planck Yearbook of United Nations Law*, vol.10, 2006, pp.264-270.

- SERGEEV A., *The right to internet access: assessing the impact and the merits of compliance through an example of modern China*, in *International Journal of Law and Information Technology*, n.25, 2017, pp.309-335.

- SHANY Y., *Toward a general margin of appreciation doctrine in International Law*, in *European Journal of International Law*, n.16, 2005, pp.927 e ss.

- SHEERAN S., RODLEY N., *Routdlege Handbook of International Human Rights Law*, Routledge, 2014, pp.381-382.

- SKEPYS B., *Is there a human right to Internet?*, in *Journal of Politics and Law*, vol.5, n.4, 2012, http://ccsenet.org/journal/index.php/jpl/article/view/22541.

- STEVENS D., O'HARA K., *Inequality.com: politics, power and digital divide*, Oxford, 2006, pp.86-87.

- TANZARELLA P., *Accesso a Internet: verso un nuovo diritto sociale?*, 3 settembre 2012, https://www.gruppodipisa.it/images/rivista/pdf/Palmina_Tanzarella__Accesso_a_Internet_verso_un_nuovo_diritto_sociale.pdf.

- VAN DJIK P. *Theory and practice of the European Convention of Human Rights*, Amsterdam, 2006.

- WU T., *Network neutrality broadband discrimination*, in *Journal on Telecommunications and High Technology Law*, vol.2, 2003, pp.141-176.

- ZENO-ZENCOVICH V., *Perché occorre rifondare il significato della libera manifestazione del pensiero*, in *Percorsi Costituzionali*, n.1, 2010, pp.69 ss.

Cap.3
Il diritto alla libera espressione nell'era cibernetica: sono necessari nuovi strumenti normativi per tutelare la libertà di parola sul web?

- BARENDT E., *Freedom of speech*, Oxford, 2007.

- BENKLER Y., *The wealth of networks: how social production transforms markets and freedom*, Yale, 2006.

- BURY BAGNELL J., *Storia della libertà di pensiero*, Milano, 1962.

- CANNIE H., VOORHOOF D., *The abuse clause and freedom of expression in the European Human Rights Convention*, in *Netherlands Quarterly of Human Rights*, n.29, 2001, pp. 54-58.

- CASTELLS M., *Communication power*, Oxford, 2009.

- CAVALIERE, P., *Digital platforms and the rise of global regulation of hate speech*, in *Cambridge International Law Journal*, vol.8 (2019) Issue 2, pp.282-304.

- COSTA P., *Motori di ricerca e social media: i nuovi filtri nell'ecosistema dell'informazione on-line e il potere occulto degli algoritmi*, in (a cura di)

AVANZINI G., MATUCCI G., *L'informazione e le sue regole. Libertà, pluralismo e trasparenza*, Napoli, 2016, pp.257.

- FISS O.M., *Why the State?*, in (a cura di) LICHTENBERG J., *Democracy and the media*, Cambridge, 1990, pp.146 ss.

- GIBBONS T., *Regulating the media*, Londra, 1998.

- GOMERY D., *Interpreting media ownership*, in (a cura di) B.M.COMPAINE, GOMERY D., *Who owns the media? Competition and concentration in the mass media industry*, Londra, 2000, pp.529 ss.

- GREER S., *The exceptions to art.8 to 11 of the European Convention on Human Rights*, https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf.

- KATSCH M.E., *The electronic media and the transformation of law*, New York, 1989.

- KELLEY D., DONWAY R., *Liberalism and free spech*, in J.LICHTENBERG, *Democracy and the media*, Cambridge, 1990, pp.81 ss.

- LAIDLAW E.B., *Regulating speech in cyberspace*, Cambridge, 2015.

- MCNAIR B., *Journalism and democracy. An evaluation of the political public sphere*, Londra, 2000.

- MCQUAIL D., *Media performance: mass comunication and the public interest*, Londra, 1992.

- MIR J.B., BASSINI M., *Freedom of expression in the Internet. Main trends of the case law of the European Court of Human Rights*, in (a cura di) O.POLLICINO, G.ROMEO, New York, NY, 2016, pp.71-94.

- MONTI M., *Fake news e social network: la verità ai tempi di Facebook*, in *Rivista del Diritto dei Media*, n.1, 2017, http://www.medialaws.eu/wp-content/uploads/2019/05/8.-Monti.pdf.

- MONTI M., *Regolazione, Internet e tecnica: le implicazioni di motori di ricerca e social networks sulla libertà di informazione*, in *Federalismi.it*, 20 dicembre 2017, https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=35322&dpath=document&dfile=17122017194247.pdf&content=Le%2Bimplicazioni%2Bdi%2Bmotori

%2Bdi%2Bricerca%2Be%2Bsocial%2Bnetworks%2Bsulla%2Blibert%C3%A0%2Bdi%2Binformazione%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B.

- NOAM E., *Two cheers for the commodification of information*, in (a cura di) ELKIN KOREN N., NETANEL N.W., *The commodification of information*, L'Aja, 2002, pp.48 ss.

- OROFINO M., *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione,* Torino, 2014.

- PARISIER E., *Filter bubble: how the new personalized web is changing what we read and what we think,* New York, 2011.

- PITRUZZELLA G., *La libertà di informazione nell'era di Internet*, in *Rivista di diritto dei media*, n.1, 2018, pp.1-28.

- POLLICINO O., BASSINI M., *Free speech, defamation and the limits to freedom of expression in the EU: a comparative analysis*, in (a cura di) A.SAVIN, J.TRZASKOWSKI, *Research Handbook on EU Internet Law*, 2014, Londra, pp.508-526.

- POLLICINO O., *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in (a cura di) BARSOTTI V., *Libertà di informazione, nuovi mezzi di comunicazione e tutela dei diritti*, Firenze, 2014, pp.101-128.

- POLLICINO O., BASSINI M., *The law of the Internet: between globalisation and localisation*, in (a cura di) MADURO M., TUORI K., SANKARI S., *Transnational law: rethinking European law and legal thinking*, Cambridge, 2014, pp.346 ss.

- PORTER V., HASSELBACH S., *Politics and the Market-place. The regulation of German Broadcasting*, Londra, 1991.

- ROZO SORDINI P.E., *La libertà di espressione nell'era digitale. Disciplina internazionale e problematiche, ISPI Working Paper*, n.52, ottobre 2013.

- SARTORI G., *Elementi di teoria politica*, Bologna, 1995, pp.174.

- SUNSTEIN C.R., *Republic.com 2.0*, Princeton, 2007.

- VAN DIJCK J., *The culture of connectivity*, Oxford, 2013.

- VILLINGER M., *Article 17 ECHR and freedom of speech in Strasbourg practice*, in (a cura di) CASADEVALL J., MVJER E., O'BOYLE M., AUSTIN A., *Freedom of expression. Essays in honour of Nicolas Bratza*, Londra, 2012, pp. 321 ss.

- VOORHOOF D., *Freedom of expression under the European Human Rights system*, in (a cura di) HAECK Y., OLASOLO H., VARVAELE J., ZWAAK L., *Inter-American and European Human Rights Journal*, 2009, pp.3-5.

- WARREN S., BRANDEIS L.D., *The right to privacy*, in *Harvard Law Review*, n.4, 1890, pp.193 ss.

- ZENO-ZENCOVICH V., *Freedom of expression. A critical and comparative analysis*, New York, 2008.

Cap.4
La privacy nell'epoca digitale: un bilanciamento tra interessi contrapposti per un'efficace tutela giurisdizionale e normativa del diritto alla riservatezza e all'autonomia informativa

- ALPA G., *La normativa sui dati personali: modelli di lettura e criteri esegetici*, in *Diritto dell'Informatica*, 1997.

- ARISTOTELE, *Politica e Costituzione di Atene*, in (a cura di) VIANO C.A., Torino, 1955.

- BERNAL P., *Internet Privacy Rights. Rights to protect autonomy*, New York, 2014.

- BYGRAVE L.A., *Data protection law: approaching its rationale, logic and limits*, Londra, 2002.

- BYGRAVE L.A., *Privacy in a global context – A comparative overview*, in *Scandinavian Studies in Law*, vol.47, 2004, pp.319-348.

- CAVOUKIAN A., *Privacy by design. The 7 foundational principles*, https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

- CIRILLO G.P., *La tutela della privacy nel sistema del nuovo codice dei dati personali*, Padova, 2004.

- D'ANTONIO V., *Oltre la cancellazione dei dati personali: l'originaria concezione del diritto all'oblio off-line*, in (a cura di) SICA S, D'ANTONIO V., RICCIO G.M., *La nuova disciplina europea della privacy*, Milano, 2016, pp.203 ss.

- D'ANTONIO V., *The right to tell people what they don't want to hear: i moderni confini del diritto di fare informazione*, in (a cura di) D'ANTONIO V., VIGLIAR S., *Studi di diritto della comunicazione. Persone, società e tecnologie dell'informazione*, Padova, 2009, pp.1 ss.

- D'ORAZIO R., *Dati personali in rete aperta*, in (a cura di) CUFFARO V., RICCIUTO V., *Il trattamento dei dati personali. Profili applicativi*, Torino, 1999, pp.276-373.

- DONNINI F.M., *L'evoluzione della protezione dei dati personali tra tecnologia, sicurezza nazionale e diritti fondamentali*, Roma, 2017.

- FABRIS F., *Il diritto alla privacy tra passato, presente e futuro*, in *Rivista di Scienze della Comunicazione*, n.2, 2009, https://www.openstarts.units.it/bitstream/10077/3394/1/09_fabris.pdf.

- FINOCCHIARO G., *Il diritto all'oblio nel quadro dei diritti della personalità,* in *Diritto dell'Informazione e dell'Informatica,* 2014, pp.593.

- FLAHERTY D., *Privacy in colonial New England*, Charlottensville, 1972.

- FROSINI V., *Il diritto nella società tecnologica*, Milano, 1981.

- GAMBINI M., *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Espaço Juridico Journal of Law*, vol.14, n.1, 2013, pp.149-190.

- GUADAMUNZ A., *Habeas data: the Latin American response to data protection*, in *Journal of Information Law and Technology*, n.1, 2000, https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz/.

- HICKSON R.F., *Privacy in a public society. Human rights in conflict*, Oxford, 1987.

- HOLVAST J., *History of privacy*, in (a cura di) K. DE LEEUW, J.BERGSTRA, *The History of Information Security: a Comprensive Handbook*, 2007, Amsterdam, pp.739 ss.

- IBBETSON D.J., *A historical introduction to the law of obligations*, Oxford, 1999.

- KONVITZ M.R., *Privacy and the law: a philosophical prelude*, in *Law and Contemporary Problems*, n.31, 1966, pp.272-281.

- KUNER C., *Reality and illusion in EU data transfer Regulation post Schrems*, in *German Law Journal*, n.18, 2017, pp.881-914.

- LAMBERT S., LINDSAY-STURGO A., *Focus on art.8 ECHR: recent developments*, in *Judicial Review*, n.13, 2008, pp.29 ss.

- LASSITER E.J., *African culture and personality: bad social science, effective social activism or a call to reinvent ethnology?* in *African Studies Quarterly*, vol.3, 2000, pp.1-21.

- MAKULILLO A.B., *"A person is a person through other persons" – A critical analysis of privacy and culture in Africa*, in *Beijing Law Review*, n.7, 2016, pp.192-204.

- MIKALSON J., *Ancient Greek religion*, Londra, 2009.

- MIRABELLI G., *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Diritto dell'Informatica,* 1997.

- MOORE JR B.., *Studies in social and cultural history*, Armonk NY, 1984.

- MUMFORD L., *La cultura delle città*, Milano, 1967.

- NEETHLING J., *The concept of privacy in South African law*, in *The South African Law Journal*, vol.122, n.1, 2005, pp. 18-28.

- NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

- NISSENBAUM H.F., *Privacy in context:technology, policy and the integrity of social life*, Stanford CA, 2010.

- PANETTA R., *Privacy by design e GDPR: un'etica per l'intelligenza artificiale,* in *Agenda Digitale*, 11 ottobre 2018, https://www.agendadigitale.eu/sicurezza/privacy/privacy-by-design-e-gdpr-unetica-per-lintelligenza-artificiale/.

- PERINAN B., *The origin of privacy as a legal value: a reflection on Roman and English law,* in *American Journal of Legal History,* vol.52, 2012, pp.183-201.

- PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016.

- POSNER R.A., *The right to privacy*, in *Georgia Law Review*, vol.12, 1978, pp.393-422.

- PROSSER W., *Privacy,* in *California Law Review,* vol.48, n.3, 1960, pp.384.

- RESTA G., *Il diritto alla protezione dei dati personali*, in (a cura di) CARDARELLI F., SICA S., ZENO-ZENCOVICH V., *Il codice dei dati personali. Temi e problemi*, Milano, 2004, pp.11-64.

- RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Bologna, 1973.

- RODOTÀ S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma, 2014.

- RODOTÀ S., *Intervista su Privacy e Libertà,* Padova, 2005.

- RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995.

- SAVIN A., *EU Internet Law*, Cheltenham, 2014.

- SCUDIERO L., *Bringing your data everywhere: a legal reading of the right to portability*, in *European Data Protection Law Review*, n.1, 2017, pp.119-127.

- SICA S., *Verso l'unificazione del diritto europeo alla tutela dei dati personali*, Cap.I, in (a cura di) SICA S, D'ANTONIO V., RICCIO G.M., *La nuova disciplina europea della privacy*, Milano, 2016, pp.5 ss.

- SOLOVE D.J., *Nothing to hide: the false tradeoff between privacyand security*, New Haven CT, 2011.

- STANZIONE M.G., *Genesi e ambito di applicazione,* Cap.II, in (a cura di) SICA S., D'ANTONIO V., RICCIO G.M., *La nuova disciplina europea della privacy*, Milano, 2016, pp.31.

- TROIANO G., *Privacy, che ci insegna la Storia sulle differenze tra Usa ed Europa*, in *Agenda Digitale*, https://www.agendadigitale.eu/sicurezza/breve-storia-della-privacy-ue-e-usa-a-confronto/.

- VALLE L., GRECO L., *Transnazionalità del trattamento dei dati personali e tutela degli interessati tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in *Diritto dell'Informazione e dell'Informatica*, fasc.2, aprile 2017, pp.168 ss.

- WARREN S.D., BRANDEIS L.D., *The right to privacy*, in *Harvard Law Review*, vol.4, n.5, 1890, pp.193-220.

- WESTIN A.F., *Privacy and freedom*, Londra, 1967.

- ZENO-ZENCOVICH V., *Il concetto di "autonomia privata" ai tempi dei "Big Data"*, in (a cura di) PASSAGLIA P., POLETTI D., *Nodi virtuali, legami informali: Internet alla ricerca delle regole*, Pisa, 2017, pp.31-37.

- ZENO-ZENCOVICH V., *Una lettura comparatistica della L.675/96 sul trattamento dei dati personali*, in *Rivista trimestrale di diritto procedurale civile*, 1998, pp.733 ss.

- ZIMMERMANN R., *The law of obligations. Roman foundations of the civilian tradition*, Oxford, 1996.