Rivista elettronica di Diritto, Economia, Management

Numero 1 - 2015 • Edizione multimediale

Atti del Convegno ANDIG
Le comunicazioni elettroniche (2014)

a cura di Donato A. Limone

FONDATA E DIRETTA DA
DONATO A. LIMONE

CLIOedu®

Direzione e redazione
Via Antonio Canal, 7
00136 Roma
donato.limone@gmail.com

Gli articoli pubblicati nella rivista sono sottoposti ad una procedura di valutazione anonima. Gli articoli sottoposti alla rivista vanno spediti alla sede della redazione e saranno dati in lettura ai referees dei relativi settori scientifico disciplinari.

Anno V, n. 1/2014
ISSN 2039-4926
Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010
Editor ClioEdu
Roma - Lecce

Indice

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2015 · pp. 9-29

Le banche dati al servizio delle piccole e medie imprese

Francesca Bailo

Multimedia

Clicca sull'immagine o fotografa il QrCode per accedere al MediaBook CLIOedu

Abstract: Il presente contributo si propone – in un'ottica prevalentemente pubblicistica – di indagare sui vantaggi e i rischi connessi all'implementazione dell'impiego delle banche dati da parte delle piccole e medie imprese, sia sotto un profilo strutturale (e, cioè, attraverso l'uso combinato di detti strumenti con il *cloud computing*), sia sotto un profilo relazionale, per la semplificazione dei rapporti con la pubblica amministrazione, con i propri dipendenti e con i propri clienti, anche alla luce del quadro normativo e giurisprudenziale di riferimento.

The aim of this article is to investigate - in a predominantly public law - the benefits and risks associated to the implementation of the use of databases by small and medium enterprises, both from a structural point of view (and, that is, through 'combined use of these tools with *cloud computing*), and in terms relational, for the simplification of relations with the public administration, with its employees and with their customers, especially in light of the regulatory and legal framework of reference.

Parole chiave: banche dati – PMI – diritto d'autore – *privacy* – sicurezza – *cloud computing* – conservazione sostitutiva – fatturazione elettronica – B.Y.O.D. – pubblicità comportamentale.

1. Premessa.

Nel presente contributo ci si propone in via preliminare di descrivere il quadro normativo e giurisprudenziale concernente le banche dati – comprensivo, dunque, non solo delle garanzie immediatamente connesse al diritto d'autore e al *diritto sui generis*, ma anche di quelle che riguardano la circolazione dei dati in esse contenuti e che determinano, principalmente, ricadute sia sulla *privacy*, sia sulla sicurezza della (e sulla) rete – per volgere quindi l'attenzione, in chiave pragmatica, ai vantaggi e alle eventuali criticità del loro impiego nelle piccole e medie imprese (d'ora in poi: PMI).
Sembra, infatti, indubbio che osservare l'implementazione di questi strumenti, specie se di carattere elettronico, dalla particolare prospettiva delle PMI, risulti di peculiare interesse in quanto pare che proprio in questo settore si possano maggiormente palesare le intrinseche capacità di pervenire, attraverso l'impiego delle ridette banche dati, non solo a ridurre costi che non sarebbero altrimenti alla portata di questa tipologia di imprese, ma anche a soddisfare esigenze che pervadono profili dell'attività (e della stessa strategia) aziendale, tali da permettere a queste ultime – o comunque contribuire notevolmente a – l'accesso, in modo competitivo, al mercato globale: e ciò sia per il caso in cui le PMI rivestano il ruolo di costitutori (magari anche in *outsourcing*), sia per il caso in cui le medesime ne fruiscano in qualità di utenti finali.
In questa prospettiva, si è perciò ritenuta opportuna la selezione di alcuni, sia pur sparsi e non esaustivi, casi di impiego delle banche dati che, proprio per i profili ora considerati, risultino di preminente rilievo, vuoi nell'organizzazione del lavoro, quando le stesse vengano usate in stretta

sinergia con tecnologie ormai sempre più capillarmente diffuse (come è per il *cloud computing*), vuoi per la possibilità che per loro tramite si semplifichino i rapporti con i diversi soggetti con cui, di volta in volta, le imprese possono venire a contatto e, quindi, sia con la pubblica amministrazione (come è per la conservazione sostitutiva in formato digitale e per la fatturazione elettronica), sia con i propri dipendenti (ciò che avviene, ad esempio, con il B.Y.O.D.), ma sia anche con i propri clienti (e, in specie, attraverso la profilazione degli utenti e la pubblicità comportamentale).
Nell'inevitabile tensione che, specie in un'ottica pubblicistica, può già anticiparsi, si registra tra interessi economici e tutela dei diritti di quanti debbano confrontarsi col fenomeno aziendale, *last but not least*, occorre precisare che, nonostante la specificità del titolo proposto, le riflessioni che seguono potranno talvolta toccare profili diversi o più ampi di quelli inerenti alle banche dati, ma che con questi appaiono variamenti connessi.

2. Le coordinate essenziali della disciplina normativa delle banche dati.

Può osservarsi, dunque, da subito che, benché le banche dati – intese come archiviazione di dati indicizzati, strutturati e collegati tra loro al fine di consentirne la gestione e l'organizzazione[1] – siano state impiegate già in epoche risalenti, la loro positiva considerazione sotto l'aspetto regolativo sia da considerarsi, tutto sommato, un fenomeno recente, e, più precisamente, allorquando, all'incirca a partire dagli anni '90 del secolo scorso[2], esse hanno iniziato ad essere utilizzate avvalendosi

[1] Sulle diverse posizioni della dottrina, italiana e straniera, in ordine alla distinzione della nozione di "banca dati" rispetto a quella di "base di dati", cfr., *ex multis*, S. Di Minico, *La tutela giuridica delle banche dati. Verso una direttiva comunitaria*, in *Inf. e Dir.*, 1996, 175 ss.

[2] Fino a quel momento, negli ordinamenti nazionali, in assenza di una specifica normativa interna, la giurisprudenza (così come, del resto, la dottrina) si era mostrata divisa tra coloro che consideravano appropriato ricomprendere le banche dati tra le opere dell'ingegno (limitando la tutela solo a quelle dotate del carattere della creatività), e coloro che ritenevano più congrua l'applicazione (in specie, per quel che riguardava il loro contenuto) della normativa sulla concorrenza sleale. Per quel che riguarda il primo orientamento, per tutti, cfr. Cass. civ., sez. I, 2 dicembre 1993, n. 11953, *Soc. Tecnodid c. Selva*, in cui la Suprema Corte, nel sostenere il carattere meramente esemplificativo (e non tassativo) di cui all'art. 2 della l. 22 aprile 1941, n. 633 (c.d. l. sul diritto d'autore), rilevò che si era in presenza di opere appartenenti alla letteratura (ai sensi dell'art. 1 della l. sul diritto d'autore), non solo quando si parlava di "opere letterarie" in senso stretto ma anche "quando la parola venga utilizzata per esprimere e comunicare dati informativi di vario genere elaborati ed organizzati in modo personale e autonomo dall'autore", nonché Pret. Roma, ord. 14 dicembre 1989, in *Foro it.*, 1990, I, 2673 ss. (con osservazioni di M. Chiarolla, *Diritto d'autore: la prima volta delle banche dati (in Italia)*, *ibidem*), che, nel sottolineare l'originalità della banca dati (su supporto elettronico) oggetto della vertenza ("frutto di un'attività di ricerca durata numerosi anni"), giunse per l'appunto a ricondurne la tutela alla disciplina prevista per il diritto d'autore. Analogamente, cfr. la sentenza della Corte suprema olandese del 4 gennaio 1991, *Van Dale Lexicografie B.V. v. Rudolf Jan Romme*, per cui una collezione di parole (nella fattispecie la copiatura e l'inserimento in una banca dati delle parole chiave di un noto dizionario olandese) avrebbe potuto essere coperta dal diritto d'autore "*if it results from a selection process expressing the author's personal views*". Per quel che riguarda il secondo orientamento, occorre osservare come le argomentazioni si basassero, fondamentalmente, su quanto disposto dall'art. 10-*bis*, n. 2, della Convenzione di Unione di Parigi del 20 marzo 1883, sulla protezione della proprietà industriale, laddove si affermava che "costituisce un atto di concorrenza

della tecnologia informatica, sì da disvelarne e massimizzarne le capacità in punto non solo di interoperabilità dei dati, ma anche di dematerializzazione.

Proprio gli interessi economici suscitati, a seguito di dette innovazioni tecnologiche, da parte delle imprese, così come la conseguente esigenza di vederne tutelati gli investimenti, del resto, hanno probabilmente indotto a una regolamentazione, propiziata, non a caso, in occasione della definizione degli *standards* internazionali per la proprietà intellettuale, contenuti nel noto *Agreement on Trade Related aspects of Intellectual Property Rights* (sez. I, art. 10, par. 2, TRIPS) e, successivamente, sempre a livello internazionale, con il Trattato WIPO sul diritto d'autore (WTC) del 20 dicembre 1996, per cui "Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such. This protection does not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation" (art. 5 WIPO).

Anche al fine di rendere competitive le PMI europee rispetto al mercato americano è, poi, come noto, intervenuta la direttiva n. 96/9/CE[3], che ha per la prima volta accordato alle banche dati una tutela "a doppio binario", la "struttura" delle stesse essendo rimessa alle garanzie proprie del diritto d'autore, e il "contenuto" essendo innovativamente protetto dal c.d. "*diritto sui generis*"[4], sulla

sleale ogni atto di concorrenza contrario agli usi onesti in materia industriale o commerciale". Con un'interpretazione ampia di detto principio, infatti, alcuni ritennero di poter inquadrare l'attività (non autorizzata) di estrazione di informazioni da una banca dati tra gli atti di concorrenza sleale, specie in seno alla *Ligue International contre la Concurrenc Deloyale*, nonché nell'A.L.A.L. (*Association Littéraire et Artistique Internationale*), affermandosi che per le banche dati non aventi i requisiti di creatività tali da poter essere ricondotte alla disciplina sul diritto d'autore "per assicurare ugualmente una protezione […] si offrono altre vie, in particolare […] le regole concernenti la concorrenza sleale", sviluppando così, specie nella giurisprudenza svizzera, ma poi anche in quella francese e olandese, la "*théories des agissements parasitaires*". Per l'applicazione del ridetto principio anche in Italia, peraltro, cfr. Trib. Genova, 4 maggio 1990, *Marconi s.r.l. c. Marchi & Marchi s.r.l.*, in *Dir. Inf.*, 1990, 1052 ss., con nota di A. Ristucci, ma anche una deliberazione dell'AGCM che sembrava volersi muovere proprio in detta direzione (delibera 10 aprile 1992, n. 452, *Ancic/Cerved*, reperibile all'indirizzo *http://www.agcm.it/ricerca-avanzata/open/41256297003874BD/0169911C2045D415C12560C3001FF7D2.html*).

[3] In ordine alle influenze esercitate da una importante sentenza della Suprema Corte americana del 27 marzo 1991, *Feist v. Rural Telephone*, sull'elaborazione della testé menzionata direttiva comunitaria, cfr., criticamente, A. Zoppini, *Privativa sulle informazioni e iniziative comunitarie a tutela delle banche dati*, in *Il dir. dell'informaz. e dell'informatica*, 1993, 895 ss., secondo cui "se era prevedibile che la sentenza americana avrebbe spiegato una significativa influenza sulla redigenda direttiva, ci si poteva attendere un atteggiamento più riflessivo da parte del legislatore di Bruxelles che non si limitasse – nell'illusione di imboccare una scorciatoia – a tradurre in norme le massime della giurisprudenza d'oltre oceano". Sul *leading case* e, in genere, sulla giurisprudenza della Suprema Corte americana in materia di banche dati, cfr. Id., *Itinerari americani ed europei nella tutela delle compilazioni: dagli annuari alle banche dati*, *ibidem*, 1992, 120 ss. Si ricordi che il caso americano, peraltro, traeva le mosse da una vertenza tra due produttori di elenchi telefonici che, pur insistendo su ambiti territoriali non perfettamente coincidenti, si contendevano il mercato pubblicitario, vertenza che fu definita dalla Corte suprema nel senso del mancato accoglimento della domanda di una delle parti di veder tutelata l'estrazione di una parte dell'elenco da parte della concorrente per il difetto dell'originalità, presupposto sulla base del quale avrebbe potuto trovare applicazione la tutela per il diritto d'autore, allora sancita dal *Copyright Act* del 1976.

[4] Si ricordi, peraltro, che, in virtù del diritto *sui generis* di cui all'art. 7 della direttiva n. 96/9/CE, si attribuisce al costitutore di una banca di dati il diritto di vietare operazioni di estrazione e/o reimpiego della totalità o di una parte sostanziale del contenuto della stessa, valutata in termini qualitativi o quantitativi, qualora il conseguimento, la verifica e la presentazione di tale contenuto attestino un investimento rilevante sotto il profilo qualitativo o quantitativo. Sul punto, e per maggiori approfondimenti, cfr., infra, alla giurisprudenza della Corte di giustizia, citata, in particolare, *infra*, alla nota 9.

cui qualificazione giuridica si è, peraltro, acceso un vivace dibattito, essendo da taluni ritenuto un diritto "connesso" alla proprietà intellettuale[5], da altri accostato alla disciplina sulla concorrenza sleale[6] e, da altri ancora, definito come un vero e proprio diritto (di privativa) "autonomo"[7] (tesi, quest'ultima, che, a quanto consta, sembra, in ultimo, essere prevalsa).

Ad ogni modo, al di là di detto ultimo profilo, che attiene ad un piano meramente dogmatico, sembra opportuno, quantomeno, segnalare che un rilevante contributo nell'interpretazione e applicazione della citata direttiva sia stato svolto dalla Corte di giustizia dell'UE che, in modo particolarmente meticoloso, si è sforzata non solo di definire alcune nozioni particolarmente dubbie sotto il profilo ermeneutico – quali, esemplarmente, il criterio dell'originalità per la tutela approntata in virtù del diritto d'autore[8], nonché i presupposti e l'oggetto della protezione del diritto *sui generis*[9] – ma ne ha anche indubbiamente esplicato le finalità e potenzialità, specie nella prospettiva della tutela di interessi e beni patrimoniali di rilievo per le imprese.

Ciò che la citata direttiva ha, viceversa, lasciato nella discrezionalità degli Stati membri, è stato il regime sanzionatorio da approntare per la violazione degli obblighi impartiti, limitandosi l'art. 12 della stessa (e, analogamente, il considerando n. 57) a raccomandare l'irrogazione di "sanzioni adeguate". In questo senso, dunque, risulta di particolare interesse osservare, da un lato, che il legislatore nazionale, all'art. 171-*bis*, comma 2, della l. 22 aprile 1941, n. 633, ha disposto al proposito alcune sanzioni penali (sia detentive, sia pecuniarie), particolarmente rigorose e, soprattutto, modulate a seconda della gravità della condotta lesiva (in senso analogo a quelle specificamente disposte per la violazione delle norme a tutela dei programmi per elaboratore), con la previsione, altresì, della confisca obbligatoria degli strumenti utili o destinati a compiere i reati ivi previsti (art. 171-*sexies*, comma 2, della l. n. 633 del 1941). Dall'altro lato, pare opportuno sottolineare che, sia pur se non proprio in riferimento alla norma incriminatrice in questione, la giurisprudenza costituzionale si è in più occasioni pronunciata sul più generale impianto sanzionatorio a difesa delle violazioni del diritto d'autore sancito nella l. n. 633 del 1941 e, almeno in certa misura, lo ha

---

[5] Al proposito, cfr. P. Spada, *"Creazione ed esclusiva", trenta anni dopo*, in *Riv. dir. civ.*, 1997, 215 ss., specc. 228 s.; G. Guglielmetti, *La tutela delle banche dati con diritto sui generis nella direttiva 96/9/CE*, in *Contr. e Impr. Europa*, 1997, 177 ss., nonché M. Cardarelli, *Il diritto sui generis: la durata*, in *Annali it. dir. autore*, 1997, 68 ss.

[6] Sul punto, cfr., peraltro, A. Zoppini, *Privativa sulle informazioni e iniziative comunitarie*, cit., 905, che, nel commentare lo schema di quella che sarebbe divenuta la direttiva n. 96/9/CE, ha rilevato che "la novità della norma va ravvisata nel fatto che consente il ricorso ad una tecnica di tipo concorrenziale indipendentemente dalla sussistenza del requisito della *confusorietà*, che sino ad oggi ha costituito – non ostante i voti espressi dalla dottrina – il principale ostacolo all'applicazione del rimedio nel sistema italiano".

[7] In questi termini, cfr. F. Ronconi, *Trapianto e rielaborazione del modello normativo statunitense: il diritto d'autore di fronte alla sfida digitale*, in G. Pascuzzi, R. Caso (curr.), *Diritti sulle opere digitali. Copyright statunitense e diritto d'autore italiano*, Padova, 2002, 283.

[8] Al proposito, e per maggiori approfondimenti, cfr. Corte di Giustizia, sent. 1° marzo 2012, nel procedimento C-604/10 (*Football Dataco e a. c. Yahoo e a.*), § 38, la quale si richiama anche a Id., sent. 16 luglio 2009, nel procedimento C-5/08 (*Infopaq c. DDF*), § 45; Id., sent. 22 dicembre 2010, nel procedimento C- 393/09 (*BSA c. Ministero ceco della Cultura*), § 50; Id., sent. 1° dicembre 2011, nel procedimento C-145/10 (*Painer c. Standard e a.*), §§ 89 e 92, che, peraltro, si sono pronunciate, in via pregiudiziale, sull'interpretazione della direttiva 2001/29/ CE, sul diritto d'autore.

[9] Al proposito, e per maggiori approfondimenti, cfr. Corte di Giustizia, sentt. 9 novembre 2004, nei procedimenti C-203/02 (*The British Horseracing Board Ltd e altri c. William Hill Organization Ltd*); C-338/02 (*Fixtures Marketing Ltd c. Svenska Spel AB*); C-444/02 (*Fixtures Marketing Ltd c. Organismos prognostikon agonon podosfairou AE (OPAP)*; C-46/02 (*Fixtures Marketing Ltd c. Oy Veikkaus Ab*), Id., sent. 5 marzo 2009, nel procedimento C-545/07 (*Apis-Hristovich EOOD c. Lakorda AD*).

giudicato congruo, ritenendolo motivato "non soltanto dalla rilevanza degli interessi coinvolti, ma anche dalla facilità e dalla diffusione dei comportamenti lesivi, soprattutto mossi da intenti lucrativi, che possono svilupparsi in un mondo ove l'opera dell'ingegno è divenuta un bene spesso di largo commercio e suscettibile di produrre cospicui profitti"[10].

Detto ciò, tuttavia, non può trascurarsi che la disciplina eurounitaria ora menzionata, recepita con il d.lgs. 6 maggio 1999, n. 169[11] e contenuta, per l'appunto, nella l. n. 633 del 1941, rappresenta solo uno, sia pur importante, dei profili che, nell'impiego delle banche dati da parte delle imprese, occorre tener presenti in quanto essa è, per lo più, improntata alla tutela dei beni patrimoniali e degli interessi economici da questi derivanti[12], ma non possono, parimenti, ignorarsi altri diritti fondamentali che, a causa della circolazione elettronica dei dati, potrebbero essere incisi e che sono, a maggior ragione, meritevoli di tutela.

A quest'ultimo proposito, vengono in rilievo, dunque, in primo luogo, la normativa, anch'essa di derivazione eurounitaria, relativa alla protezione dei dati personali e della vita privata nel settore delle comunicazioni elettroniche e, in secondo luogo e più in generale, le azioni e le strategie adottate, a vari livelli, per la garanzia della sicurezza della (e sulla) rete, principalmente a contrasto del *cyber crime*, ulteriori rispetto alle responsabilità individuali già contemplate all'art. 615-*ter* c.p, derivanti da accessi abusivi a sistemi informatici e telematici (in cui sono senza dubbio ricomprese le banche dati elettroniche).

Per quel che riguarda il primo versante, occorre quantomeno segnalare che detti svolgimenti normativi, così come la loro tutela, sono stati particolarmente riguardati, oltreché a livello giurisprudenziale, dal Garante per la protezione dei dati personali nazionale che, con provvedimenti e deliberazioni, di carattere sia generale, sia particolare, ha avuto il merito di fare chiarezza su alcuni

---

[10] In questo senso, cfr. Corte cost., sent. 28 febbraio 1997, n. 53. Già in precedenza, cfr. Corte cost., sent. 17 aprile 1968, n. 23, secondo cui "Dal complesso delle norme contenute nella legge in esame, fino al titolo quinto […] risulta, quindi, in modo non equivoco, che il legislatore ha ritenuto la tutela e l'esercizio del diritto di autore di tale rilevanza di interesse generale, e, quindi, pubblico, da non esitare a prevedere particolari forme di reato, che, espressamente, sono predisposte ad assicurarne la difesa". In senso analogo, cfr., poi, Id., sent. 19 aprile 1972, n. 65; Id., sent. 5 luglio 1973, n. 110; Id., ord 24 marzo 1988, n. 361; Id., sent. 6 aprile 1985, n. 108.

[11] Sul punto, peraltro, cfr. anche l'art. 43 della legge comunitaria annuale per gli anni 1995-1997 (l. 24 aprile 1998, n. 128), con cui il Governo era stato delegato a dare attuazione alla direttiva n. 96/9 CE secondo i seguenti principi e criteri direttivi: a) definire la nozione giuridica di banca di dati ai sensi dell'articolo 1 della direttiva ed agli effetti del recepimento della medesima; b) comprendere la banca di dati, alle condizioni previste dalla direttiva, tra le opere protette ai sensi dell'articolo 2 della legge 22 aprile 1941, n. 633, e successive modificazioni; c) riconoscere e disciplinare l'esercizio del diritto esclusivo dell'autore delle banche di dati; d) prevedere deroghe al diritto esclusivo di autorizzare l'estrazione e il reimpiego di una parte sostanziale del contenuto di una banca di dati, in conformità a quanto disposto dall'articolo 6, comma 2, lettere b) e c), della direttiva stessa; e) riconoscere e disciplinare, in applicazione delle disposizioni contenute nel capitolo III della direttiva, il diritto specifico di chi ha costituito la banca di dati alla tutela dell'investimento; f) prevedere disposizioni transitorie in conformità a quanto previsto dall'articolo 14 della direttiva.

[12] Obiettivo, quest'ultimo, peraltro, analogo, a quello che ispira la normativa approntata per i programmi per elaboratori che, parimenti, ha trovato una protezione negli accordi e trattati internazionali menzionati, nonché, a livello eurounitario, in una direttiva, la n. 91/250 CEE (ora abrogata e sostituita dalla direttiva n. 2009/24 UE), che, di fatto, ha funzionato da modello per la disciplina afferente alle banche dati "creative" e che, nella prassi, trova spesso applicazione insieme a quest'ultima, in quanto i ridetti programmi per elaboratore vengono utilizzati anche per la costituzione o il funzionamento di banche di dati accessibili grazie a mezzi elettronici.

casi pratici di spiccato interesse per le PMI operanti nel settore[13], su cui si avrà modo di portare l'attenzione nel prosieguo.

Per quel che riguarda il secondo versante, inoltre, riservandoci di approfondirne alcuni profili nella disamina della casistica selezionata, basti, poi, esemplarmente, osservare che, anche in virtù delle strategie sulla *cybersecurity* impartite a livello eurounitario, alcune misure di preminente rilievo sono state adottate a livello nazionale per la sicurezza della rete con l'intenzione, tra l'altro, di individuare specifiche azioni a supporto delle PMI, da ultimo, nel Quadro strategico nazionale per la sicurezza dello spazio cibernetico (la cui adozione è stata comunicata con il d.p.c.m. 27 gennaio 2014)[14]. In detta sede, infatti, ci si propone di individuare "i profili e le tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale", e di specificare ruoli e compiti dei diversi soggetti pubblici e privati – ivi comprese le PMI, che si vorrebbe supportare con servizi di pubblica assistenza e collaborazione – oltreché di definire "strumenti e procedure con cui perseguire l'accrescimento delle capacità del Paese di prevenire e rispondere in maniera compartecipata alle sfide poste dallo spazio cibernetico".

3. Le banche dati, le PMI e l'organizzazione dell'attività d'impresa: il cloud computing.

Negli ultimi dieci anni, è stata portata avanti l'idea di introdurre, nel campo dell'informatica, l'offerta di tecnologia come mero "servizio", tanto da superarsi la tradizionale vendita di beni e prodotti su supporti fisici, quali *hardware* e *software*, e consentire, così, "la disponibilità e accessibilità ai propri dati in ogni momento, gratuitamente o a costi estremamente ridotti, da qualunque dispositivo collegato alla rete"[15].

---

[13] *Ex multis*, cfr. il provvedimento di carattere generale del 12 marzo 2009 (reperibile all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1598808*) con cui il Garante per la protezione dei dati personali, nel dare puntuali prescrizioni ai titolari del trattamento dei dati in possesso di banche dati costituite sulla base di elenchi telefonici prima del 1° agosto 2005 e che intendessero utilizzarle per fini promozionali, è stato fatto obbligo di trattare direttamente i ridetti dati personali ivi presenti, senza possibilità di cederli ad alcuno. Lo stesso Garante ha poi provveduto ad emettere ordinanze di ingiunzione alle PMI non attenutesi alle dovute prescrizioni, con l'irrogazione di sanzioni amministrative pecuniarie particolarmente considerevoli. Al proposito, cfr., ad es., l'ordinanza di ingiunzione dell'8 maggio 2014 (all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3275922*) e, in precedenza, le ordinanze di ingiunzione del 15 marzo 2012 (all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2115627*) e il provvedimento inibitorio del 26 giugno 2008 (all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1544315*). In senso analogo, cfr. anche un altro provvedimento inibitorio del 25 settembre 2008, relativo ad una fattispecie di impiego delle banche dati dei *call center* (all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1562758*).

[14] Il ridetto Quadro strategico è reperibile all'indirizzo *http://www.governo.it/backoffice/allegati/74839-9250.pdf*.

[15] In questo senso, cfr. G. Troiano, *Profili civili e penali del cloud computing nell'ordinamento giuridico nazionale: alla ricerca di un equilibrio tra diritti dell'utente e doveri del fornitore*, in *Cyberspazio e diritto*, 2011, XII, 234. Sono queste, dunque, le principali caratteristiche del *cloud computing*, che, in estrema sintesi, consiste "in un insieme di tecnologie e risorse informatiche, accessibili direttamente *on-line* grazie allo sviluppo delle reti di comunicazione, autonomamente predisposto e controllato dall'impresa ovvero alla stessa fornito da terzi sotto forma

Non stupisce, dunque, come detto innovativo e ormai diffuso modello, meglio noto con il termine "*cloud computing*" sia, in primo luogo, funzionale al salvataggio dei dati in *server* esterni all'azienda e virtualizzati in rete e, perciò, sia spesso (se non proprio inevitabilmente) combinato con l'impiego di banche dati elettroniche, e, in secondo luogo, possa risultare di particolare interesse per l'implementazione delle politiche aziendali delle PMI, visto che, in tal modo, gli obiettivi a cui le stesse potrebbero pervenire grazie all'uso delle sole banche dati, sono, in qualche modo, esaltati, con il venire "offerti servizi aventi lo *standard* delle grandi imprese, dei quali non potrebbero fruire se dovessero contare solamente sulle proprie risorse *in house*"[16].

Le implicazioni economiche da ciò derivanti, hanno, dunque, probabilmente indotto le istituzioni, a livello sia eurounitario, sia nazionale, ad adottare alcune importanti strategie e azioni volte, da un lato, ad accrescerne l'utilizzo e, dall'altro lato, ad affrontarne e prevenirne le criticità.

Già nel 2010 un gruppo di esperti ha redatto un rapporto per la Commissione europea sul "Futuro del *cloud computing*"[17], a cui è seguito uno specifico atto della Commissione (Comunicazione COM (2012) 529 del 27 settembre 2012[18]), che, ponendosi l'obiettivo di sfruttare il potenziale della ridetta tecnologia in Europa ha, tra l'altro, sottolineato che l'adozione di detto servizio da parte delle PMI "con tutta probabilità determinerà un forte miglioramento dell'efficienza nell'economia globale", specie "in economie in difficoltà o in regioni periferiche o rurali" che, così, potranno accedere ai mercati di regioni "più dinamiche". Grazie a infrastrutture a banda larga, si consentirà, cioè, a tutti gli operatori, dalla *start-up* ad alta tecnologia ai piccoli commercianti o artigiani, di "sfruttare la nuvola per accedere a mercati lontani", raggiungendosi anche "la massa critica necessaria per negoziare condizioni di favore con *partner* commerciali importanti (ad es. fornitura/trasporto, operatori turistici e imprese finanziarie)".

In senso analogo, uno studio elaborato dalla Direzione generale politiche interne presso il Parlamento UE[19], ha rilevato che *il cloud computing* può essere considerato come "una forma potenziata e flessibile di esternalizzazione da parte di un'impresa o un'organizzazione" per la sua capacità di ridurre "le spese generali per la gestione informatica" e di consentire, al contempo, "un consoli-

di servizio" (in questo senso, cfr. A. Mantelero, *Processi di outsourcing e cloud computing: la gestione dei dati personali e aziendali*, in *Il dir. dell'informaz. e informatica*, 2010, 673). Peraltro, sul punto, cfr. anche la definizione fornita dal National Institute Standards and technology (NIST), secondo cui "is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud). Key enabling technologies include: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware".

[16] In questo senso, cfr. A. Mantelero, *Processi di outsourcing e cloud computing*, cit., 676.

[17] Il ridetto rapporto è reperibile, in lingua inglese, all'indirizzo *http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1175*.

[18] La comunicazione è reperibile all'indirizzo *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:it:PDF*.

[19] Il citato studio è reperibile all'indirizzo *http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_IT.pdf*.

damento e un'ottimizzazione su larga scala delle risorse *hardware* e s*oftware* di calcolo", in quanto, "invece che investire capitale per l'acquisto di attrezzature costose, le imprese devono semplicemente assegnare *budget* operativi per «noleggiare» l'accesso ai servizi di cui hanno bisogno in un dato momento". Secondo quanto si rileva nel citato studio, il risultato è, cioè, quello di "uniformare le condizioni del contesto competitivo, rendendo le risorse di calcolo su grande scala per la prima volta disponibili alle piccole imprese e alle altre organizzazioni che non hanno un'adeguata infrastruttura (comprese, a livello macro, le economie in via di sviluppo, almeno per quelle regioni che hanno già un'infrastruttura a banda larga sufficientemente affidabile e veloce); ancora, "a livello di fornitore di servizi *cloud*, l'aggregazione appianerebbe i picchi e minimi nella variabilità della domanda, consentendo tassi di sfruttamento dei *server* più elevati". Aggiungendosi che i servizi *cloud* possono supportare tutti i tipi di applicazioni e servizi delle imprese, coprendo, cioè, l'intero spettro delle esigenze aziendali: dalla pianificazione della continuità dell'attività alla gestione dei picchi di domanda, fino a un servizio completamente esternalizzato, oltre a permettere di "collegare i processi aziendali di numerosi fornitori diversi e migliorare la collaborazione tra diversi reparti all'interno della stessa organizzazione".

Sono state, inoltre, definite alcune strategie (quali, esemplarmente, l'*EU Cloud Initiative*, e l'*eGovernment Action Plan* 2011 – 2015) facenti capo all'Agenda digitale europea e la stessa Agenzia per l'Italia digitale nazionale partecipa sia a gruppi che contribuiscono allo sviluppo di *standard* di livello europeo nel settore, sia a interessanti progetti di ricerca dedicati, quali il "*Cloud for Europe*"[20] e il "*Coco Cloud*"[21].

Da un punto di vista prettamente legislativo, tuttavia, l'implementazione del *cloud computing* ha riguardato solo l'ambito della pubblica amministrazione[22], mentre spunti di maggior interesse, nella prospettiva delle PMI, a livello interno, provengono da una scheda di documentazione elaborata dal Garante per la protezione dei dati personali su "*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*"[23], rivolta specificamente "a tutti gli utenti di dimensioni contenute e di limitate risorse economiche (singoli, piccole o medie imprese, amministrazioni locali quali i piccoli comuni, ecc.) destinatari della crescente offerta di servizi di *cloud computing* (pubbliche o ibride), con l'obiettivo di favorire l'adozione consapevole e responsabile di tale tipologia di servizi".

A fronte degli innumerevoli vantaggi ora posti in luce e delle strategie approntate, come emerge negli stessi studi e atti, di livello nazionale e sovranazionale, citati, non può, tuttavia, sottacersi che le PMI, e in genere, le imprese che si approcciano a detta nuova tecnologia, potrebbero trovarsi esposte a talune difficoltà di cui occorre dare, almeno succintamente, conto.

Una prima difficoltà riguarda, infatti, la stessa applicabilità delle regole sul diritto d'autore, coinvolgenti all'evidenza sia i programmi per elaboratore attraverso cui il servizio viene reso, sia le banche dati attraverso cui il ridetto servizio viene posto in essere. Essendo, per l'appunto, il *software*

---

[20] Per maggiori informazioni su detto progetto, cfr. all'indirizzo *http://www.cloudforeurope.eu/*.

[21] Per maggiori informazioni su detto progetto, cfr. all'indirizzo *http://www.coco-cloud.eu/*.

[22] Al proposito, cfr. l'art. 47, comma 2-*bis*, lett. *d)* del d.l. 9 febbraio 2012, n. 5 (conv., con modif., dalla l. 4 aprile 2012, n. 35), nonché l'art. 68, comma 1, lett. *d)* del d.lgs. 7 marzo 2005, n. 82, così come modificato dall'art. 9-*bis* del d.l. 18 ottobre 2012, n. 179 (conv., con modif., dalla l. 17 dicembre 2012, n. 221).

[23] La citata scheda di documentazione, pubblicata congiuntamente alla relazione annuale 2010, è reperibile all'indirizzo *http://194.242.234.211/documents/10160/10704/1819933*.

distribuito non già come un bene (su supporto fisico), ma come un servizio, l'opera dell'ingegno resta "installata sul computer del fornitore e visualizzabile dall'utente attraverso un'interfaccia grafica", così che, fatta forse eccezione per il *cloud* Iaas (in cui i fornitori licenziano le c.d. "istanze virtuali")[24], "la possibilità che il titolare del diritto d'autore possa «licenziare» i propri diritti risulta inattuabile perché il *software* non è distribuito" e "il sistema è strutturato in modo che sia il fornitore a controllarlo"[25]. Ciò che non esclude (ma, anzi, almeno in certa misura rafforza) la "non sicurezza" del *software* stesso, specie laddove esso, come spesso accade, nasconda al suo interno "vulnerabilità per finalità eticamente molto discutibili"[26].

Altri problemi potrebbero, poi, insorgere per il trasferimento dei dati tra *data center* diversi, dislocati in luoghi spesso non noti all'utente. Oltre all'introduzione di elementi di quasi sicura "internazionalità", solo in parte arginati dalla previsione di cui all'art. 45 del d.lgs. n. 196/2003 – con cui è disposto che, fuori dei casi di cui agli artt. 43 e 44 del medesimo d.lgs., il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato, a tal proposito dovendosi valutare anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza – particolari difficoltà, infatti, parrebbero registrarsi per quel che attiene alla sicurezza dei dati.

La scrupolosità con cui le misure, anche tecniche[27] (previste, in particolare, dagli artt. 31 e ss. del d.lgs. n. 196/2003[28], nonché dal disciplinare tecnico di cui all'allegato B al ridetto Codice), dovreb-

---

[24] Si ricordi che il clous IaaS (acronimo che sta per *Infrastructure as a Service*) si caratterizza (rispetto ai *cloud PaaS e SaaS*) per il fatto che in detta circostanza l'utente può acquistare risorse di memorizzazione (*Storage Cloud)* o computazionali (*Compute Cloud*) in quantità proporzionate alle proprie esigenze. Sul punto, e per maggiori approfondimenti, G. Troiano, *Profili civili e penali del cloud computing nell'ordinamento giuridico nazionale*, cit., 235, nota 11, nonché A. Mantelero, *Processi di outsourcing e cloud computing,* cit., 682 s.

[25] In questo senso, cfr. G. Troiano, *Profili civili e penali del cloud computing nell'ordinamento giuridico nazionale*, cit., 246. Sul punto, peraltro, cfr. anche C. Flick, *Dati nelle nuvole: aspetti giuridici del cloud computing e applicazione alle amministrazioni pubbliche*, in *Federalismi* (all'indirizzo *http://www.federalismi.it*), 20 marzo 2013, 7 s., per cui "la riunificazione di dati nelle mani di singoli operatori di mercato che non intervengono nel mettere a disposizione su internet opere creative ma che si limitano a consentirne la diffusione richiede, sotto il profilo della tutela dell'autore dell'opera, la necessità di abbattere l'ampio ambito di irresponsabilità del fornitore del servizio, che consente a quest'ultimo di non rispondere per i contenuti caricati dagli utenti. È evidente, infatti, la difficoltà per l'autore dell'opera di individuare i singoli che, in ipotesi, abbiano violato i suoi diritti (alla quale si aggiungono problemi di coordinamento con la disciplina in materia di privacy) e costi considerevoli che un'indagine su singoli soggetti comporterebbe".

[26] In questo senso, cfr. G. Troiano, *Profili civili e penali del cloud computing nell'ordinamento giuridico nazionale*, cit., 247.

[27] Al proposito, cfr., in particolare, l'art. 34, lett. *e)* e *f)*, del d.lgs. n. 196/2003, con cui si impone l'adozione di misure di sicurezza in ordine sia alla protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici, sia per l'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi. Ipotesi, queste ultime, che, in caso di violazione, comportano l'irrogazione delle sanzioni penali di cui all'art. 169 del medesimo d.lgs. n. 196/2003.

[28] Peraltro, con un provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (*c.d. data breach*) del 4 aprile 2013 (all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2388260*), il Garante per la protezione dei dati personali ha chiarito che i fornitori di servizio a cui sono impartiti gli obblighi di cui all'art. 32-*bis* del d.lgs. n. 196/2003, sono definibili come coloro che, essenzialmente, offrono il servizio telefonico e l'accesso a internet, specificando, dunque, che nessun obbligo è, esemplarmente, imposto, al proposito, nel caso in cui la

bero essere adottate, talora da parte delle stesse PMI, se si vuole, potrebbero essere aggravate dalle difficoltà derivanti dalla compresenza di elementi di internazionalità nei rapporti, il che, purtroppo, induce a porre in discussione la presunzione della riduzione dei costi aziendali che detta tecnologia mirerebbe ad agevolare e, dunque, la stessa possibilità per le PMI di accedere, per questa via, ad un mercato più "dinamico".

Su questo profilo, soprattutto in riferimento ai cd. *big data*, ossia uno dei servizi dell'ICT in forte espansione[29], sta, comunque, portando una particolare attenzione la Commissione europea, nello sforzo di attenuare, quando sarà adottato il nuovo Regolamento dell'Unione in materia di *privacy*[30], l'attuale complessità del quadro giuridico e le conseguenti difficoltà di accedere a grandi *dataset* e alle infrastrutture abilitanti: l'obiettivo apertamente dichiarato è proprio quello di eliminare le barriere che ostacolano l'ingresso sul mercato delle PMI che dovrebbero essere, invece, le prime generatrici di innovazione, e di colmare il divario attuale tra investimenti degli operatori europei e americani[31].

violazione riguardi "una banca dati del fornitore che non attiene in maniera specifica al servizio offerto dallo stesso, ma ad una qualunque delle altre attività che svolge, ad esempio alla gestione del personale o alla contabilità". Del pari, non vi rientrano:
a)"coloro che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche)", in quanto i servizi non sono "accessibili al pubblico"; né
b) "i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso a Internet utilizzando tecnologia senza fili, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale"; né, ancora,
c) "i gestori dei siti Internet che diffondono contenuti sulla rete (c.d. "*content provider*"), a meno che non offrano anche il servizio di posta elettronica, limitatamente alla gestione dei dati personali relativi allo stesso, per i quali rientrano viceversa nel campo di applicazione della nuova disciplina"; né, in ultimo,
d) "i gestori di motori di ricerca, salvo l'eventuale componente di trasmissione dati".
Parimenti, per "terzi affidatari del servizio", a cui sono impartiti gli obblighi di comunicazione di cui all'art. 32-*bis* del d.lgs. n. 196/2003, devono intendersi esclusivamente gli "operatori virtuali di rete mobile (MVNO)" e, in ultima analisi, "le società che forniscono servizi di telefonia mobile senza possedere alcuna licenza per il relativo spettro radio né tutte le infrastrutture necessarie per fornire tali servizi e che utilizzano a tale scopo una parte dell'infrastruttura di uno o più operatori mobili reali" e che "sono dotati di archi di numerazione telefonica propri e quindi di proprie SIM card, possono gestire in proprio le funzioni di commutazione e di trasporto nonché la base dati di registrazione degli utenti mobili. Sono, quindi, completamente autonomi nella relazione con i clienti, i quali non hanno alcun rapporto diretto con l'operatore di rete mobile e stipulano un unico contratto, appunto, con il MVNO". Sul punto, e per maggiori precisazioni, cfr. anche la delibera dell'Autorità per le garanzie nelle comunicazioni n. 544/00/CONS, "*Condizioni regolamentari relative all'ingresso di nuovi operatori nel mercato dei sistemi radiomobili*" (pubblicata in G.U. n. 183 del 7 agosto 2000, all'indirizzo *www.gazzettaufficiale.it/eli/id/2000/08/07/00A11171/sg*).

[29] Più precisamente, si tratta dell'elaborazione di enormi ed eterogenee quantità di dati al fine della loro compattazione in *dataset* di considerevoli dimensioni. Al proposito, e per maggiori approfondimenti, cfr., *infra*, in questa *Rivista*, G. Crea, *Il ruolo delle reti di comunicazione elettronica di nuova generazione nella prospettiva dell'open (big) data*.

[30] In argomento, e per maggiori approfondimenti, cfr., *infra*, in questa *Rivista*, M. Cuniberti, *Le comunicazioni elettroniche alla luce del nuovo regolamento europeo in materia di identificazione elettronica*.

[31] Lucidamente in questo senso, A. Gambino, relazione al convegno *Governance di Internet ed efficienza delle regole: verso il nuovo regolamento europeo sulla privacy*, svoltosi il 13 novembre 2014 a Roma e organizzato dall'Accademia Italiana per il Codice di Internet (*paper*).

4. Le banche dati, le PMI e la semplificazione dei rapporti aziendali: conservazione sostitutiva dei dati, fatturazione elettronica e B.Y.O.D.

Gli effetti positivi dell'uso delle banche dati da parte delle PMI si esplicano non solo in vista dell'ottimizzazione dell'organizzazione dell'attività di impresa, ma anche a mezzo della semplificazione dei rapporti con i principali soggetti che vengono, pressoché quotidianamente, a contatto con le stesse PMI e, dunque, *in primis*, la pubblica amministrazione, ma poi anche i propri dipendenti e i consumatori finali.

In questo senso, e con riguardo al primo dei rapporti considerati, particolarmente dirimente sembra l'incremento, proprio grazie all'impiego delle banche dati, della gestione documentale informatizzata dei dati che, peraltro, impone, anche alle PMI che vogliano perseguire detta finalità, il rispetto di almeno le "regole tecniche" definite con il d.p.c.m. 3 dicembre 2013 che, nell'abrogare la delibera Cnipa 19 febbraio 2004, n. 11, ha avuto come esito quello di rendere i processi di dematerializzazione più strutturati e complessi, anche alla luce dell'introduzione di un nuovo *standard*, di una nuova ISO (l'*Open archival information system*) e del modello UNIsincro. A fronte di dette maggiori incombenze, peraltro, è stato emanato il DMEF 17 giugno 2014[32] che, nell'abrogare il DMEF 23 gennaio 2004, si propone di armonizzare le disposizioni di legge o di regolamento di natura tributaria sulla conservazione con le citate regole tecniche, avendo, quantomeno, il merito di introdurre semplificazioni importanti al processo di dematerializzazione della documentazione fiscale[33] tali da offrire maggiore slancio e diffusione dei processi di conservazione digitale già a partire dal periodo d'imposta 2015.

Ciò a maggior ragione in seguito al recente e correlato obbligo della fatturazione elettronica[34]

---

[32] Il testo del ridetto DMEF, pubblicato nella G.U. n. 146 del 26 giugno 2014, è reperibile all'indirizzo *www.gazzettaufficiale.it/eli/id/2014/06/26/14A04778/sg*.

[33] Tra le novità introdotte con il citato DMEF, vi sono, esemplarmente, l'eliminazione dell'obbligo di conservazione quindicinale delle fatture (ora allineato a quello della tenuta dei libri e dei registri), tenuto conto che il processo di conservazione dei documenti con valenza fiscale deve essere effettuato entro il termine previsto dall'art. 7, comma 4-*ter*, del d.l. 10 giugno 1994, n. 357 (conv., con modif., nella l. 8 agosto 1994, n. 489) e, quindi, entro tre mesi dal termine della presentazione della dichiarazione dei redditi; e l'espunzione dell'obbligo di comunicazione dell'impronta dell'archivio dei documenti con rilevanza tributaria all'Agenzia delle entrate, dovendo il contribuente comunicare l'effettuazione della conservazione in modalità elettronica dei ridetti documenti già nella dichiarazione dei redditi relativa al periodo di imposta di riferimento. Inoltre, l'art. 4 del ridetto DMEF dispone che «ai fini tributari il procedimento di generazione delle copie informatiche e delle copie per immagine su supporto informatico di documenti e scritture analogici avviene ai sensi dell'art. 22, comma 3, del decreto legislativo 7 marzo 2005, n. 82, e termina con l'apposizione della firma elettronica qualificata, della firma digitale ovvero della firma elettronica basata sui certificati rilasciati dalle Agenzie fiscali».

[34] Per una prima definizione, cfr. l'art. 21 del d.P.R. 26 ottobre 1972, n. 633, per cui per "fattura elettronica si intende la fattura che è stata emessa e ricevuta in un qualunque formato elettronico". Sul punto, cfr., poi, la circolare dell'Agenzia delle entrate del 3 maggio 2013, n. 12/E e, in ultimo, quella del 24 giugno 2014, n. 18/E (all'indirizzo *http://www.agenziaentrate.gov.it/wps/file/nsilib/nsi/documentazione/provvedimenti+circolari+e+risoluzioni/circolari/archivio+circolari/circolari+2014/giugno+2014/circolare+n18e+del+24+giugno+2014/cir18e+del+24+06+14.pdf*), relativa anche ai processi di fatturazione elettronica tra imprese.

verso la pubblica amministrazione[35], che si svolge anch'essa attraverso l'impiego prevalente delle banche dati. Su quest'ultimo versante, infatti, è stato emanato il d.m. 3 aprile 2013, n. 55[36], con cui sono state adottate non solo le "regole tecniche" relative alle modalità di emissione della fattura elettronica, nonché alla trasmissione e al ricevimento della stessa attraverso lo SdI (allegato B al regolamento), ma anche le "misure di supporto" per le PMI, stabilendosi che il Ministro dell'economia e delle finanze renda loro disponibili in via non onerosa sul proprio portale elettronico "i servizi e gli strumenti di supporto di natura informatica in tema di generazione delle fatture nel formato previsto dal Sistema di Interscambio e di conservazione, nonché i servizi di comunicazione con il detto Sistema", mentre, per parte sua, l'Agenzia per l'Italia digitale (in collaborazione con Unioncamere e sentite le associazioni di categoria delle imprese e dei professionisti) deve mettere a disposizioni delle PMI, sempre in via non onerosa, il supporto per lo sviluppo di strumenti informatici "*open source*" (art. 4 del D.M. n. 55 del 2013)[37].

Emerge, così, con maggior nitidezza, l'esigenza, anche per le PMI (come già per le pubbliche amministrazioni), di affidare dette attività ad una figura professionale specializzata, ossia al "responsabile della conservazione sostitutiva", visto anche che, secondo quanto disposto dall'art. 12, comma 2, del d.p.c.m. 3 dicembre 2013, i soggetti privati appartenenti ad organizzazioni che già adottano specifiche regole di settore per la sicurezza dei sistemi informativi devono adeguare il sistema di conservazione alle misure ivi meglio dettagliate, mentre gli altri soggetti possono adottare quale modello di riferimento le regole di sicurezza indicate dagli articoli 50-*bis* e 51 CAD (oltre alle relative linee guida emanate dall'Agenzia per l'Italia digitale) e i sistemi di conservazione devono rispettare le misure di sicurezza previste dagli artt. 31 e ss., nonché dal disciplinare tecnico di cui all'allegato B, del d.lgs. n. 196/2003.

Venendo, poi, rapidamente, al secondo dei rapporti considerati, e cioè a quello con i propri dipendenti, spunti per una semplificazione, attraverso l'impiego delle banche dati in formato elettronico, per le imprese in genere, e per le PMI in particolare, sembrano derivare dall'ormai esponenziale

---

[35] Come noto, infatti, l'obbligo della fatturazione in formato elettronico, in dette circostanze, è stato introdotto con la legge finanziaria 2008 (art. 1, comma 209, della l. 24 dicembre 2007, n. 244, così come modificato dall'art. 10, comma 13-*duodecies* del d.l. 6 dicembre 2011, n. 201, conv., con modif., nella l. 22 dicembre 2011, n. 214), e riguarda, per l'appunto, l'emissione, la trasmissione, la conservazione e l'archiviazione delle fatture emesse nei rapporti con la P.A. Attività, queste ultime, che devono svolgersi nell'osservanza di quanto disposto dal d.lgs. 20 febbraio 2004, n. 52 (di attuazione della direttiva 2001/115/CE, sulla semplificazione ed armonizzazione delle modalità di fatturazione in materia di IVA), nonché dello stesso CAD, e tenendo conto che la trasmissione dovrebbe avvenire attraverso il SdI (Sistema di Interscambio). Al proposito, cfr. il d.m. del 7 marzo 2008, che ha individuato l'Agenzia delle Entrate quale gestore del Sistema di Interscambio e la Sogei quale apposita struttura dedicata ai servizi strumentali ed alla conduzione tecnica.

[36] Sul punto, cfr., poi, la Circolare del Ministero dell'economia e delle finanze del 31 marzo 2014, n. 1 (all'indirizzo *http://www.finanze.gov.it/export/download/novita2014/2014-03-31_Circolare_FE.pdf*).

[37] Occorrerà, dunque, attendere che il nuovo regime entri pienamente in funzione (essendo fissata al 31 marzo 2015 l'estensione generalizzata a tutta la pubblica amministrazione dell'obbligo di adozione della fatturazione elettronica) e verificare se le regole (anche di natura tecnica) approntate presentano o meno criticità ancora tutte da vagliare. Sembrerebbe, in ogni caso, di poter anticipare che detto strumento, così come, in genere, la conservazione sostitutiva in formato digitale, possa contribuire notevolmente a semplificare il rapporto delle PMI con la pubblica amministrazione e renderlo maggiormente trasparente, limitandosi al minimo i rischi che non siano quelli della sicurezza della rete, che, peraltro, sembrano poter essere abbastanza efficacemente fronteggiati attraverso l'istituzione di personale altamente specializzato e le agevolazioni offerte proprio a dette imprese.

sviluppo dei fenomeni B.Y.O.D. (acronimo che sta per "*bring your own device*", ma ci sono anche altre varianti: *bring your own technology* (B.Y.O.T.), *bring your own phone* (B.Y.O.P), e *bring your own* PC (B.Y.O.PC)) e Consumerizzazione IT, che paiono rappresentare la naturale evoluzione del più tradizionale telelavoro[38], con l'imporsi di un modello di lavoratore "nomade" che si muove grazie alla sempre più capillare disponibilità di una connessione a banda larga e alla sempre maggiore portabilità dei propri strumenti tecnologici (quali *smartphone* e *tablet*), permettendo di esercitare la propria attività in remoto – e, nella maggior parte dei casi, in *cloud* – e di accedere, quindi, alle applicazioni aziendali[39].

Occorre, tuttavia, sottolineare che, se dette innovazioni, collocabili nel più ampio *frame* dello *smart work*, hanno sicuramente il pregio di migliorare l'organizzazione complessiva degli uffici e dei posti di lavoro, oltreché di ottimizzare la qualità delle prestazioni (spesso a vantaggio delle categorie più deboli), comportano anche ineluttabili – e, almeno in certa misura, amplificati – rischi, più o meno mediati, sulla *privacy*, sulla sicurezza, sulla proprietà intellettuale e, in ultimo, sulle stesse strategie aziendali.

Pur non essendoci, ad oggi, una normativa *ad hoc* sul punto[40], occorre quantomeno segnalare che

---

[38] Si ricordi che il telelavoro è stato introdotto nel nostro ordinamento con l'art. 4 della l. 16 giugno 1998, n. 191 (a cui è stata data attuazione con D.P.R. 8 marzo 1999, n. 70 e con l'Accordo Quadro del 23 marzo 2000) in riferimento alla sola pubblica amministrazione, mentre, nel settore privato, la regolamentazione, in recepimento dell'Accordo quadro europeo del 16 luglio 2002, è stata affidata all'Accordo interconfederale del 9 giugno 2004, i cui principi sono stati poi eventualmente adeguati e/o integrati dalla contrattazione collettiva. Con l'art. 22, comma 5, della l. 12 novembre 2011, n. 183 (Legge di stabilità 2012) sono, inoltre, state individuate alcune misure volte a favorire il telelavoro, con particolare riguardo ai lavoratori disabili e in mobilità e, da ultimo, nel d.d.l. delega sul c.d. *Jobs act* (nella versione approvata definitivamente dal Senato in data 3 dicembre 2014 e non ancora pubblicato : A.S. 1428-B), all'art. 1, comma 9, lett. *d*), allo scopo di garantire un adeguato sostegno alla genitorialità, si prevede l'indicazione al Governo di criteri e principi direttivi tesi all'incentivazione di accordi collettivi volti a promuovere la flessibilità dell'orario lavorativo e dell'impiego di premi di produttività, al fine di favorire la conciliazione tra l'esercizio delle responsabilità genitoriali e dell'assistenza alle persone non autosufficienti e l'attività lavorativa, anche attraverso il ricorso al telelavoro.

[39] Sulle applicazioni intelligenti, scaricabili sui propri dispositivi mobili, e sui rischi per la privacy degli utenti, cfr., *amplius*, il parere 2/2013 del WP29 del 27 febbraio 2013 (all'indirizzo *http://www.privacy.it/grupripareri201302.html*).

[40] Occorre, tuttavia, quantomeno segnalare che è stata presentata una proposta di legge presso la Camera dei Deputati (l'A.C. del 29 gennaio 2014, n. 2014, di iniziativa dell'on. Mosca e a.), recante "*Disposizioni per la promozione di forme flessibili e semplificate di telelavoro*", già oggetto di consultazione pubblica e di pubblicazione *on-line*, che si propone l'obiettivo di configurare lo *smart work* come strumento e non come tipologia contrattuale, "con lo scopo di renderlo utilizzabile da tutti i lavoratori che svolgano mansioni compatibili con questa possibilità, anche in maniera «orizzontale» […] a seconda dell'accordo raggiunto tra datore di lavoro e lavoratore, attraverso una modifica alla normativa in materia di Agenda digitale, per estendere gli incentivi fiscali alle aziende che adottano dette modalità di lavoro "agile". Nella citata proposta di legge, più nel dettaglio, all'art. 4, si dispone che il datore di lavoro adotti "misure atte a garantire la protezione dei dati utilizzati ed elaborati dal lavoratore che svolge la propria prestazione lavorativa in regime di *smart working*" e che, per sua parte, il lavoratore sia tenuto "a custodire con diligenza tutte le informazioni aziendali ricevute, anche tramite gli strumenti informatici o telematici eventualmente utilizzati", detto obbligo estendendosi anche "alle apparecchiature fornite dal datore di lavoro, che devono essere custodite in modo da evitare il loro danneggiamento o smarrimento", mentre, all'art. 5, si stabilisce che il datore di lavoro debba essere considerato "responsabile della fornitura e della manutenzione degli strumenti informatici o telematici eventualmente utilizzati dal lavoratore", salvo che abbia pattuito con il lavoratore la messa a disposizione di strumenti informativi e tecnologici di proprietà di quest'ultimo e, soprattutto, che "al fine di verificare il rispetto dei criteri di proporzionalità

di detti profili problematici si sono, almeno in parte, fatti carico l'ENISA[41], per quel che concerne il fronte della sicurezza, e il Garante per la protezione dei dati personali, per quello della *privacy*. In particolare quest'ultimo è intervenuto con l'individuare alcune interessanti "*Linee guida in tema di riconoscimento biometrico e firma grafometrica*" adottate il 21 maggio 2014[42] in cui è stato, tra l'altro, rilevato che, nell'ambito della crescente diffusione, nei più importanti settori produttivi, di modelli di lavoro fortemente caratterizzati da mobilità abbinata a interazione con i sistemi informativi aziendali, un trattamento biometrico effettuato con dispositivi mobili (es. *tablet*), "può andare incontro, in assenza di adeguate e specifiche misure di sicurezza, a rischi maggiori rispetto allo svolgersi del trattamento all'interno del perimetro di sicurezza aziendale", specie laddove "l'accentuata possibilità di uso promiscuo dello strumento e, addirittura, dell'uso personale e familiare, per motivi ludici e ricreativi, non si concilia con la sicurezza dei dati anche in considerazione dell'accresciuta esposizione al rischio e all'utilizzo di applicativi non selezionati e installabili in modo incontrollato dall'utente". Sottolineandosi, del resto, che raramente, in questi contesti, "vengono adottati meccanismi di controllo degli accessi anche di tipo basilare, come il blocco automatico per inattività, né vengono offerte modalità di connessione sicura con protocolli avanzati per proteggere i dati in mobilità che rimangono esposti poiché trasmessi su canali insicuri"[43].

e di pertinenza dell'eventuale controllo", il datore di lavoro debba inviare un'informativa generale alla direzione territoriale del lavoro del luogo dove ha sede l'azienda, nella quale deve descrivere le caratteristiche tecniche degli strumenti informatici o telematici forniti al lavoratore. Quest'ultima, ricevuta l'informativa, deve, dunque, "verificare l'entità, la proporzionalità e la pertinenza degli eventuali controlli che le caratteristiche tecniche degli strumenti informatici o telematici forniti al lavoratore possono consentire al datore di lavoro, tenendo conto della necessità di permettere all'azienda e al lavoratore di utilizzare sistemi efficaci di collegamento nell'ambito di una prestazione lavorativa che si caratterizza, tra l'altro, per l'essere resa al di fuori dei locali aziendali" e, in presenza di eventuali motivi ostativi, essa può chiedere nei successivi trenta giorni chiarimenti in relazione ai medesimi strumenti informatici o telematici, dando un termine non superiore a quindici giorni per la risposta. La ridetta procedura dovrebbe concludersi, "in ogni caso", entro quarantacinque giorni dall'invio della prima informativa, con l'applicazione del principio del silenzio assenso (dovendosi considerare equivalente all'autorizzazione di cui all'art. 4 della l. 20 maggio 1970, n. 300, con la precisazione non è necessaria in caso di accordo sottoscritto con le rappresentanze sindacali aziendali).

41 Al proposito, cfr., in particolare, il rapporto "*Consumerization of IT: Final report on Risk Mitigation Strategies and Good Practices*" del 19 dicembre 2012, all'indirizzo *http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COIT_Mitigation_Strategies_Final_Report/at_download/fullReport*.

42 Dette Linee guida sono reperibili all'indirizzo *http://www.garanteprivacy.it/garante/document?ID=3132361*.

43 Nello "schema di provvedimento in tema di riconoscimento biometrico e firma grafometrica (reperibile all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3132642*) adottato unitamente alle menzionate Linee guida, poi, è stato rilevato che l'utilizzo di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici è soggetto a una crescente diffusione, tra gli altri, per l'accesso a banche dati informatizzate aziendali, e, per tale ragione, è stata rimarcata l'esigenza che, anche per essi siano osservate, in generale, le disposizioni del Codice (e, in particolare, quelle di cui all'art. 17) poiché "l'adozione di sistemi biometrici, in ragione della tecnica prescelta, del contesto di utilizzazione, del numero e della tipologia di potenziali interessati, delle modalità e finalità del trattamento, comporta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato". In questa prospettiva, tra l'altro, si è raccomandato che, nella circostanza in cui sistemi di firma grafometrica vengano utilizzati nello scenario mobile o B.Y.O.D. (*Bring Your Own Device*), debbano "essere realizzati idonei sistemi di gestione dei dispositivi mobili (sistemi MDM – *Mobile Device Management*) per isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di *software* anche nel caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (*malware*)".

Se, dunque, per la tutela di detti profili, qualcosa si sta muovendo, sembra non essere ancora compiutamente emersa e/o stata approfondita un'altra criticità, ossia quella degli aspetti del *licensing* per il B.Y.O.D., in quanto la maggior parte di fornitori di *software* e banche dati non hanno ancora definito come si possano acquisire regolarmente licenze d'uso per strumenti aziendali da eseguirsi però su dispositivi di proprietà del dipendente, né sembrano dipanarsi del tutto i profili di responsabilità che da ciò potrebbero derivarne, tenuto conto che si tratterebbe pur sempre di uso di strumenti informatici personali in ambito aziendale.
Si tratta, in ogni caso, di una rivoluzione – sia nel mondo del lavoro, sia, più ampiamente, nell'ambito delle tecnologie informatiche – che sembra destinata a protrarsi nel tempo e che, alla luce delle numerose implicazioni che presenta su almeno alcuni dei diritti fondamentali sopra menzionati, è, dunque, meritevole di essere attentamente "monitorata", in attesa di prossimi (e, probabilmente necessari) sviluppi sotto un profilo normativo.

5. Le banche dati, le PMI e la semplificazione dei rapporti con la clientela: pubblicità comportamentale e profilazione dei dati.

È ampiamente noto come attraverso motori di ricerca, generici o specializzati, *social network* e sistemi di geolocalizzazione[44] sia ormai diventato piuttosto semplice, con l'indicizzazione e l'aggregazione dei dati, addivenire ad una profilazione, più o meno dettagliata, degli internauti – in grado di definire delle vere e proprie "identità digitali" – così come è del pari evidente che, per ognuna di dette attività, un ruolo fondamentale venga svolto dalle banche dati[45].
Ciò che più preme, tuttavia, in questa sede sottolineare è che dette informazioni, nella prospettiva delle PMI, possono essere utili non solo a condurre ricerche di mercato, ma anche ad attivare quello che è un vero proprio *marketing* di prossimità, sì da porle in grado di orientarsi sul "come" fare pubblicità e a quale "*target*" rivolgersi.
La pubblicità comportamentale, in particolare, diversamente dalle pubblicità contestuali o segmentate (che ricorrono a "istantanee" di ciò che gli internauti visualizzano o fanno su un particolare sito *web*, oppure a caratteristiche note degli utenti), si basa "sull'osservazione del comportamento

---

[44] Su quest'ultimo profilo, per maggiori approfondimenti, anche in una prospettiva comparata, cfr., in dottrina, per tutti e più recentemente, P. Costanzo, *Note preliminari sullo statuto giuridico della geolocalizzazione (a margine di recenti sviluppi giurisprudenziali e legislativi)*, in *Il diritto dell'informaz. e dell'informatica*, 2014, 331 ss.

[45] Esemplarmente, attraverso la geolocalizzazione, compaiono spesso sul proprio dispositivo (grazie ad autorizzazioni rilasciate alle applicazioni più o meno inconsapevolmente scaricate), le condizioni meteorologiche e i "punti di interesse" vicini al luogo in cui ci si trova, ma può anche capitare che, sulla semplice base di ricerche effettuate su motori di ricerca generici e l'incrocio di detti dati con la corrispondenza scaricata tramite *e-mail*, si attivino sulla schermata del proprio fornitore di comunicazione (e, più nello specifico, nella "*home*") informazioni sugli *hobbies* e i luoghi già visitati in precedenza dall'utente sul *web*, nonché quelli più "affini" ai primi. Sulla pagina personale dei *social network* più noti, compare poi un "*banner*" con la pubblicità dei prodotti, dei locali, degli alberghi, dei luoghi o delle "*stars*" su cui gli "amici" hanno indicato la propria preferenza.

delle persone nel tempo" attraverso le loro azioni (frequentazione ripetuta di certi siti, interazioni, parole chiave, produzione di contenuti online, ecc.), con lo scopo di elaborare un profilo specifico e quindi inviare messaggi pubblicitari che corrispondano perfettamente agli interessi dedotti. Così, vede coinvolti, essenzialmente, i fornitori di rete pubblicitaria (con la funzione di "monitorare" gli utenti e tracciarne il comportamento attraverso le tecnologie di *targeting* – principalmente grazie ai *cookie* ma anche agli ancor più invasivi *fingerprinting* – e le banche date connesse, ai fini della distribuzione), spesso in partenariato con i fornitori di accesso a internet (in quanto in grado di inserire *tracking cookie* in tutto il traffico *web* non criptato), l'editore (che ha il compito di riservare sul proprio sito *web* uno spazio per la visualizzazione del messaggio pubblicitario) e l'impresa (che attraverso i dati messi a disposizione dal fornitore di rete pubblicitaria, negozia con l'editore per porre in essere il c.d. marjeting di prossimità).
Lo *streaming* di dati ottenuti, idonei a consentire di "seguire" ogni momento della vita dell'internauta, e, in certa misura, di condizionarne le scelte, se, da un lato, rappresenta una fonte di guadagno importante, specie per le PMI e, in genere, permette la crescita e l'espansione dell'economia *on-line*, dall'altro lato, porta, tuttavia, inevitabilmente, a sollevare significative preoccupazioni per la (talora indebita) interferenza nella sfera privata di ogni individuo che necessariamente comporta.
Di tali ultime criticità, oltreché il legislatore eurounitario (con le note direttive nn. 95/46 CE, 2002/58 CE e, da ultimo, 2009/136 UE[46]), e il Consiglio d'Europa[47], si è fatto particolarmente carico il Gruppo di lavoro sull'art. 29 (WP29), prima con il parere 2/2010[48], sulla pubblicità comportamentale *online* e successivamente – a seguito della definizione di un "codice di autoregolamentazione delle buone prassi in materia di pubblicità comportamentale online" redatto dai maggiori operatori coinvolti (*l'European Advertising Standards Alliance* (EASA) e l'Internet Advertising Bureau Europe (IAB)[49] – con il parere n. 16/2011, con cui si è, peraltro, rilevata la non perfetta aderenza dell'approccio di *opt-out* suggerito nel ridetto codice di autoregolamentazione con la normativa eurounitaria.
Sul piano nazionale, poi, di un certo interesse risultano alcuni provvedimenti adottati dal Garante per la protezione dei dati personali che – pur avendo, in genere, come destinatari sia i fornitori di servizi di comunicazione, sia i gestori di motori di ricerca generici o di siti – riguardano, sia pur incidentalmente, le stesse PMI e che, pur appuntandosi tutti sugli obblighi degli operatori coinvolti

---

[46] Per maggiori approfondimenti sulle citate direttive, nonché sulla normativa di recepimento nazionale, con particolare riferimento al fenomeno della pubblicità comportamentale e al *marketing* diretto, cfr. A. Mantelero, *Si rafforza la tutela dei dati personali:* data breach notification *e limiti alla profilazione mediante i* cookies, in *Il dir. dell'informaz. e dell'informatica*, 2012, 4-5, 781 ss. Si ricordi, viceversa, che la direttiva 2006/24/CE, sulla conservazione dei dati personali di traffico telefonico e telematico, è stata recentemente dichiarata invalida dalla stessa Corte di giustizia, con la ormai nota sent. 8 aprile 2014, nelle cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd contro Irlanda*, su cui, per tutti, cfr., in dottrina, O. Pollicino, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi*, 24 novembre 2014 (all'indirizzo *http://www.federalismi.it*).

[47] Al proposito, cfr., in particolare, la raccomandazione CM/Rec(2010)13 del Comitato dei ministri presso il Consiglio d'Europa del 23 novembre 2010, su "*the protection of individuals with regard to automatic processing of personal data in the context of profiling*".

[48] Al proposito, cfr. il parere 2/2010 sulla "*pubblicità comportamentale online*", adottato il 22 giugno 2010 (all'indirizzo *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_it.pdf*).

[49] Il citato codice di comportamento è reperibile all'indirizzo *http://www.easaalliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf/download*

in merito all'esigenza dell'ottenimento di un consenso effettivamente informato degli utenti e, perciò, sulla necessità di un mutamento della stessa filosofia con cui essi operano sul mercato digitale (talora travalicando in quello che è, piuttosto, un "mercato virale" o un vero e proprio "*social spam*"[50]), hanno, comunque, sottolineato la strategicità della pubblicità comportamentale, specie nell'economia delle imprese di piccole o medie dimensioni.

Il riferimento è, esemplarmente, ad un provvedimento generale del 25 giugno 2009[51], con cui si è, tra l'altro, verificato che i fornitori di servizi di comunicazione elettronica accessibili al pubblico effettuano, in genere "attività di profilazione utilizzando dati personali che vengono anche aggregati secondo parametri predefiniti individuati da ciascun titolare di volta in volta, a seconda delle esigenze aziendali". Dette attività di profilazione possono, così, comprendere "informazioni personali di tipo variegato, tra cui dati di carattere contrattuale e dati relativi ai consumi effettuati, dai quali è possibile desumere indicazioni ulteriori riferibili a ciascun interessato (ad esempio, fascia di consumo, livello di spesa sostenuto ad intervalli regolari, servizi attivi su ciascuna utenza)" e, dunque, sono potenzialmente in grado di permettere la disponibilità e trattabilità dei dati, seppur su base aggregata, così da rendere disponibile "un patrimonio informativo che va ben al di là delle informazioni considerate singolarmente e relative a ciascun interessato", al fine di "monitorare l'andamento economico della società o, eventualmente, in un secondo momento, anche di progettare e realizzare campagne di *marketing* sulla base delle analisi effettuate"[52].

Analoghe osservazioni sono state poi ribadite, di recente, sia in un altro provvedimento generale

---

[50] Fenomeni, questi ultimi, che, peraltro, hanno reso necessaria l'adozione, con provvedimento del Garante per la protezione dei dati personali del 4 luglio 2013, di apposite "*Linee guida in materia di attività promozionale e contrasto allo spam*" (all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2542348*) e di un provvedimento generale del 15 maggio 2013, recante "*Consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto*" (all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2543820*). Particolarmente secondo le citate Linee guida, dunque, per "*social spam*" deve intendersi "un insieme di attività mediante le quali lo spammer veicola messaggi e link attraverso le reti sociali online", e, in quanto tale è sottoposto alla disciplina di cui agli artt. 3, 11, 13, 23 e 130 del Codice. Esso deve considerarsi illecito particolarmente nel caso in cui l'utente riceva, in privato, in bacheca o nel suo indirizzo di posta e-mail collegato al suo profilo social, un determinato messaggio promozionale relativo a uno specifico prodotto o servizio da un'impresa che abbia tratto i dati personali del destinatario dal profilo del social network al quale egli è iscritto, a meno che il mittente non dimostri di aver acquisito dall'interessato un consenso preventivo, specifico, libero e documentato ai sensi dell'art. 130, commi 1 e 2, del Codice. Per "*marketing virale*", invece, sempre secondo dette Linee guida, deve intendersi "una modalità di attività promozionale mediante la quale un soggetto promotore sfrutta la capacità comunicativa di pochi soggetti destinatari diretti delle comunicazioni per trasmettere il messaggio ad un numero elevato di utenti finali" e, in genere, con detta locuzione vuole farsi riferimento "agli utenti di Internet che suggeriscono o raccomandano ad altri l'utilizzo di un determinato prodotto o servizio". Detta attività, quando viene svolta con modalità automatizzate e per finalità di *marketing*, può rientrare nello spam se non rispetta le già menzionate norme di cui agli artt. 3, 11, 13, 23 e 130 del Codice. Su detti profili, in ogni caso, per maggiori approfondimenti, si rinvia a M. Farina, *Comunicazioni elettroniche commerciali e protezione dei dati personali: linee guida in materia di attività promozionale e contrasto allo spam*, *infra*, in questa *Rivista*.

[51] Il riferimento è, in particolare, al provvedimento su "*Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione - 25 giugno 2009*", all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1629107*.

[52] Ciò che ha condotto alla definizione di una serie dettagliata di prescrizioni, a pena dell'irrogazione delle sanzioni previste dal d.lgs. n. 196/2003, in particolare per la violazione degli obblighi sull'informativa degli utenti e la prestazione del consenso al trattamento dei propri dati personali.

sugli obblighi dei gestori di siti facenti uso di *cookie*[53], sia in un provvedimento individuale nei confronti del motore di ricerca generico Google[54], adottato anche alla luce della nota pronuncia della Corte di giustizia sul diritto all'oblio implicato, tra l'altro, dagli artt. 7 e 8 della Carta di Nizza-Strasburgo[55], e all'apposita istruttoria compiuta, proprio a seguito di detta pronuncia, dallo stesso WP29[56]. Provvedimento, quest'ultimo, in cui, peraltro, è emerso come la stessa "filosofia" imprenditoriale della società – tesa a voler offrire ai propri utenti un servizio unificato mediante l'integrazione e l'interoperabilità di diversi prodotti e funzionalità, anche al fine di fornire agli interessati una migliore esperienza di utilizzo – non sia conforme al dettato normativo, in specie in ragione del fatto che "le operazioni di trattamento tese alla profilazione dell'utente anche per scopi di analisi e di monitoraggio dei visitatori di siti *web* nonché all'invio di pubblicità personalizzata realizzate anche attraverso l'incrocio di dati raccolti in relazione a funzionalità diverse", non rientrano nei casi di esonero dall'obbligo di acquisizione del consenso di cui all'art. 24 del Codice[57].

---

[53] Il riferimento è, in particolare, al provvedimento generale dell'8 maggio 2014 (*Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014*", all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884*). Al proposito, e per maggiori approfondimenti, cfr., in dottrina, S. Cavalcanti, *Cookies: Italian Data Protection Authority's New Rules Information Notice and Consent*, in *Federalismi*, 19 settembre 2014 (all'indirizzo *http://www.federalismi.it*).

[54] Il riferimento è al "*Provvedimento prescrittivo nei confronti di Google Inc. sulla conformità al Codice dei trattamenti di dati personali effettuati ai sensi della nuova privacy policy*", del 10 luglio 2014 (all'indirizzo *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3283078).* Tra le criticità segnalate in detto provvedimento, di peculiare interesse, ai nostri fini, risulta quella della "omessa richiesta del consenso degli interessati per finalità di profilazione tesa anche alla visualizzazione di pubblicità comportamentale personalizzata ed all'analisi e monitoraggio dei comportamenti dei visitatori di siti *web*, nonché mancato rispetto del diritto di opposizione degli interessati". Ipotesi, questa, ritenuta in contrasto con gli artt. 7, 23, 24 e 122 del d.lgs. n. 196/2003, in quanto effettuata mediante:
"a) trattamento, in modalità automatizzata, dei dati personali degli utenti autenticati in relazione all'utilizzo del servizio per l'inoltro e la ricezione di messaggi di posta elettronica […];
b) incrocio dei dati personali raccolti in relazione alla fornitura ed al relativo utilizzo di più funzionalità diverse tra quelle messe a disposizione dell'utente;
c) utilizzo di *cookie* e altri identificatori (credenziali di autenticazione, *fingerprinting* etc.), necessari per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso delle funzionalità offerte (*pattern*)".
Si ricordi, peraltro, che analoghi provvedimenti sono stati adottati anche dai Garanti nazionali di Francia, Germania, Regno Unito, Paesi Bassi e Spagna.

[55] Il riferimento è, in particolare a Corte di giustizia, sent. 13 maggio 2014, nella causa C-131/12, *Google Spain c. AEPD.* Per un commento alla citata decisione, in dottrina, cfr., per tutti, O. Pollicino, *Interpretazione o manipolazione?*, cit., nonché G.E. Vigevani, *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano*, in *Federalismi,* 19 settembre 2014 (all'indirizzo *http://www.federalismi.it*).

[56] Al proposito, cfr., il *Press Release* del WP 29 del 6 giugno 2014, reperibile all'indirizzo *http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140606_wp29_press_release_google_judgment_en.pdf*. Si ricordi, peraltro, che il ridetto gestore, in seguito al Press Release e alla citata pronuncia della Corte di Giustizia del 13 maggio 2014, ha messo a disposizione un *tool* per consentire agli utenti di avanzare le relative istanze di cancellazione.

[57] Occorre, peraltro, aggiungere, per maggior completezza, che, in detto provvedimento individuale, si è precisato, altresì, che il ricorso a tecniche di identificazione diverse dai *cookie* basato "sul trattamento, da parte della società, di dati personali ovvero anche di informazioni o parti di informazioni (che non sono o non sono ancora dati personali ma che, poste in associazione tra loro ovvero con altre informazioni, possono diventarlo), con l'obiettivo di pervenire all'identificazione inequivoca (cd. *single out*) del terminale e, per il suo tramite, anche del profilo di uno o più utilizzatori di quel dispositivo", deve, più propriamente, essere denominato *fingerprinting*. Detta tecnica si caratterizza, perciò, per la visualizzazione di pubblicità comportamentale personalizzata e per l'analisi e il monitoraggio dei comportamenti dei

Nuovi spunti di riflessione nella definizione di un congruo bilanciamento tra i diritti degli operatori del settore a far uso delle tecnologie offerte dalle banche dati e, in genere, dal *targeting*, per addivenire, attraverso una profilazione degli internauti, ad un *marketing* di prossimità e agli opposti – ma non necessariamente contradditori – diritti di tutela della riservatezza dei propri dati personali (ivi compreso, se si vuole, il diritto all'oblio in essi implicato), da un lato, e all'indicizzazione e al diritto di "apparire", dall'altro lato (che, si badi, potrebbe coinvolgere anche le persone fisiche, al di là di interessi strettamente economici), sembrano, peraltro, provenire dalla proposta di regolamento sulla protezione generale dei dati, laddove, esemplarmente, si dispone che il responsabile del trattamento debba fornire all'interessato informazioni "chiare ed evidenti" in ordine al trattamento dei propri dati a fini di profilazione, indicando ad esso, altresì, il diritto di opporsi (obblighi, questi, il cui rispetto è reso cogente anche in virtù di sanzioni – al più amministrative – modulate e proporzionate, particolarmente, alla condotta tenuta), e si affida all'istituendo comitato europeo per la protezione dei dati il compito di emettere orientamenti, raccomandazioni e buone prassi, per specificare ulteriormente i criteri e le condizioni per la profilazione[58]. Previsioni, queste ultime, analoghe a quelle, per ora solo abbozzate, inserite nella Dichiarazione dei diritti in internet da parte della Commissione per i diritti e i doveri relativi ad Internet istituita in seno alla Camera dei deputati nel luglio 2014 e presieduta dal prof. Rodotà[59].

visitatori di siti *web*, ma, rispetto ai *cookie* – in cui l'utente che non intenda essere profilato, oltre alle tutele di carattere giuridico connesse all'esercizio del diritto di opposizione, ha anche la possibilità pragmatica di rimuoverli direttamente (in quanto archiviati all'interno del proprio dispositivo) – non pone rimedi sufficienti a tutela dell'interessato, considerato che il solo strumento nella disposizione del medesimo "consiste nella possibilità di rivolgere una specifica richiesta al titolare, confidando che essa venga accolta", in contrasto con i requisiti richiesti dagli artt. 23, 24 e 122 del d.lgs. n. 196/2003.

[58] Non sono, viceversa, stati approvati gli emendamenti proposti dalla Commissione per l'industria, la ricerca e l'energia del 26 febbraio 2013, nn. 38 e 182 (rispettivamente relativi al considerando n. 58 e all'art. 20 del regolamento, così come individuati nella proposta originaria della Commissione del 25 gennaio 2012) che si proponevano, da un lato, di escludere dall'ambito di applicazione del regolamento l'attività di profilazione mediante trattamento automatizzato i cui effetti reali non fossero paragonabili, per intensità, agli effetti giuridici, ivi essendo espressamente incluse le misure relative alla comunicazione commerciale, quali, ad esempio, le misure nel settore della gestione delle relazioni con i clienti o dell'acquisizione della clientela e, dall'altro lato, di chiarire che ai fini del *marketing*, della ricerca di mercato o dell'adeguamento dei mezzi di comunicazione telematica alle esigenze, fosse possibile realizzare profili di utilizzo impiegando dati pseudonomizzati, purché l'interessato non si fosse opposto, al precipuo scopo di evitare che, nel raccogliere un consenso per ogni forma di trattamento, si ponessero le condizioni per "distruggere il modello aziendale di innumerevoli piccole e medie imprese europee, avvantaggiando in tal modo le grandi aziende degli Stati Uniti". Peraltro, occorre precisare che, sia pur se non nei medesimi termini, l'idea di "allentare" gli obblighi imposti al responsabile del trattamento in caso di pseudonomizzazione dei dati raccolti è stata almeno in parte accolta nel progetto da ultimo approvato dal Parlamento in data 12 marzo 2014 (all'indirizzo *http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=IT&ring=A7-2013-0402*), prevedendosi (con l'emendamento n. 34, che introduce il considerando 58-*bis*) la presunzione per cui "la profilazione basata esclusivamente sul trattamento dei dati pseudonimi non incida significativamente sugli interessi, sui diritti o sulle libertà dell'interessato", e precisandosi che, qualora la profilazione, sia essa basata su una singola fonte di dati pseudonimi o sull'aggregazione dei dati pseudonimi da diverse fonti, consenta al responsabile del trattamento di attribuire i dati pseudonimi a un soggetto specifico, "i dati trattati non vanno più considerati pseudonimi" e, quindi, necessitano del consenso dell'interessato.

[59] Sul punto, e per maggiori approfondimenti, cfr., *infra*, in questa *Rivista*, F. Faini, *La rete e lo scontro fra diritti: diritto all'informazione, diritto d'autore e privacy nell'era dei byte*, nonché G. Scorza, *Internet bill of rights: una proposta da discutere*.

6. Qualche breve osservazione conclusiva.

Si confida di esser riusciti a mettere a fuoco non tanto quanto più banalmente è facile constatare e cioè che l'utilizzo da parte delle PMI delle banche dati elettroniche, nelle loro varie declinazioni ed evoluzioni, ha costituito e costituisce uno straordinario salto di qualità ed opportunità rispetto alle tradizionali strategie aziendali industriali e commerciali e uno strumento per aver accesso e rimanere su un mercato fino ad ora egemonizzato da strutture aziendali più importanti e di livello internazionale, ma che (ed è ciò che maggiormente rileva) questa stessa circostanza sia stata presa in carico dal legislatore nazionale ed europeo come ulteriore incentivo allo sviluppo di un'economia globale, nel rispetto e nella garanzia di un mercato libero e aperto e nel contempo "tutelato". Obiettivo, quest'ultimo, che, peraltro, in una dimensione costituzionale, non può non tener conto, da un lato, dell'ormai mutato (e costantemente *in fieri*) scenario tecnologico e, dall'altro lato, dell'esigenza di una dialettica tra la tutela dei diritti prettamente patrimoniali che conseguono al sempre più capillare impiego delle banche dati, ormai da tempo garantiti dalla proprietà intellettuale latamente intesa (e, quindi, comprensiva delle garanzie apprestate con il diritto *sui generis*), con una ancor più diffusa e uniforme tutela dei diritti della persona (e della personalità), nella più ampia prospettiva di quella che va costruendosi come una vera e propria identità digitale all'interno di un società che non è più solo locale ma che, anzi, ha un impatto sempre più transfrontaliero.