LUISS Law Review

N. 2/2017

INDICE

PARTE PRIMA

ARTICOLI

PARTE SECONDA

DOSSIER MONOGRAFICO

CYBER SECURITY, DIGITAL PRIVACY & ARTIFICIAL INTELLIGENCE

SEZIONE PRIMA: CYBER SECURITY

SEZIONE SECONDA: DIGITAL PRIVACY & ARTIFICIAL INTELLIGENCE

LUISS Law Review

LUISS Law Review - Rivista online del centro di ricerca LUISS DREAM, Dipartimento di Giurisprudenza LUISS Guido Carli
Registrata presso il Tribunale di Roma con il n. 65/2016
ISSN 2531-6915
Direttore responsabile: Gian Domenico Mosco
Responsabile di redazione: Raffaella Scarabino
LUISS Guido Carli - Viale Pola, 12, 00198 Roma, Italia P.I. 01067231009

Parte prima

Articoli

L'applicazione dell'articolo 102 TFUE alle azioni inibitorie su "standard essential patents"

di **CARLO MEO**

Abstract

One of the most hotly debated competition law topics is the application of antitrust rules to standards and, more specifically, to injunctions on standard essential patents. A peculiar feature of this debate is the opposition between different views both within the academic literature and between national judges and the European Commission practice. Eventually, the questions raised by the standard setting scenario have reached the CJEU scrutiny, through the referral carried out by German judges in the *Huawei* case. Therefore, the CJEU ruling is an occasion to analyze the application of article 102 TFEU to standard essential patents. An interesting aspect of the decision is that the European Court of Justice regards the injunction for SEPs as a form of "derivative" abuse, based on a previous abusive refusal to license. Moreover, so called "*de facto*" standards are not included in the scope of the *Huawei* ruling, although their features do not appear to justify a different treatment under 102 TFEU. It also seems then that the *Huawei* ruling will raise a new wave of uncertainty, instead of setting a clear solution to the problem of injunctions, since it places the concept of FRAND at the very heart of the test. An alternative way of applying article 102 TFEU is proposed in the last part of the work.

1. Introduzione. Uno degli argomenti più dibattuti in materia di diritto industriale è l'applicazione delle disposizioni antitrust agli standard di produzione e, più in particolare, all'esercizio dei brevetti coinvolti nella definizione delle norme tecniche. Il dibattito ha visto contrapposte non solo varie voci all'interno della dottrina giuridica ed economica ma anche i giudici nazionali e la Commissione europea. Le questioni sono, infine, giunte

all'attenzione della Corte di Giustizia, attraverso il deferimento pregiudiziale proposto dai giudici tedeschi nella vicenda *Huawei*. La sentenza della Corte di Giustizia è dunque l'occasione, colta in questo scritto, per esaminare l'applicazione dell'art. 102 TFUE ai brevetti essenziali negli standard di produzione.

2. Il fallimento delle negoziazioni. La standardizzazione produttiva è il fenomeno per cui imprese concorrenti, attraverso incontri svolti in apposite organizzazioni, si accordano per uniformare un certo aspetto dei propri prodotti[1]. Nella maggior parte dei casi, ciò che spinge le imprese a "standardizzare" la produzione è la ricerca di modalità tecniche di comunicazione tra i rispettivi prodotti (c.d. interoperabilità)[2]. Lo sviluppo o, addirittura, l'esistenza di certi mercati dipende dall'interazione tra i prodotti e dalla loro interoperabilità tramite soluzioni tecniche uniformi (SHAPIRO 2001, 81)[3].

1 In UE il fenomeno è riconosciuto ufficialmente, protetto e fortemente incentivato: si v. per un'utile ricostruzione del sistema europeo di standardizzazione: COMMISSIONE EUROPEA, *Independent Review of the European Standardization System: Final Report,* 2015, disponibile sul sito: http://ec.europa.eu/growth/single-market/european-standards/notification-system_it. Si v. anche, per un confronto con lo sviluppo del fenomeno negli Stati Uniti, ZENO-ZENCOVICH, 2007, 5 ss. Da ultimo, si v. il REGOLAMENTO N. 1025/2012 del Parlamento Europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea. E' stata recentemente pubblicata una "roadmap" relativa alle prossime iniziative della Commissione Europea in materia di standard con l'obiettivo di rendere più semplice l'identificazione e la valutazione dei brevetti coinvolti negli standard: COMMISSIONE EUROPEA, *Standard essential patents for a European digitalised economy,* 10 aprile 2017, disponibile su https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-1906931_en.

2 L'interoperabilità dei prodotti non sempre è raggiunta attraverso il lavoro di organismi di standardizzazione. Esistono infatti tecnologie che, di fatto, si affermano e si diffondono sul mercato fino a diventare indispensabili per operare in un certo settore industriale; si ha dunque uno standard c.d. "di fatto". V. a tal proposito Causa C-418/01, *IMS Health,* 29 aprile 2004, par. 12. Gli standard cui ci si riferisce nel testo sono detti "*de iure*" e si distinguono da quelli "di fatto" perché sono fissati su accordo degli operatori di un settore industriale, anziché per il successo ottenuto sul mercato. Per il fatto che sono il frutto della cooperazione tra imprese operanti nello stesso settore, gli standard "*de iure*" possono sollevare problemi antitrust ai sensi dell'articolo 101 TFUE: si v. al riguardo le *Linee Direttrici sull'Applicabilità dell'Articolo 101 del Trattato sul Funzionamento dell'Unione Europea agli Accordi di Cooperazione Orizzontale*, 2011/C 11/01, par. 264 e ss., dove la Commissione esamina dettagliatamente il tema dell'applicazione dell'articolo 101 TFUE agli standard "*de iure*" (anche detti "accordi di standardizzazione" o "accordi di normazione").

3 La necessità di interoperabilità tra i prodotti è evidente nel settore delle telecomunicazioni. Si tenga presente che la maggior parte degli standard di produzione riguarda proprio il settore c.d.

Nei settori ad alto contenuto tecnologico, come quello delle telecomunicazioni, gli standard consistono in soluzioni tecniche complesse e si fondano su innumerevoli invenzioni coperte da brevetti[4]. Le invenzioni in questione sono indispensabili per l'applicazione dello standard. Ogni operatore che intenda partecipare al mercato dei prodotti aderenti allo standard deve ottenere le licenze per l'utilizzo dei relativi brevetti, che vengono, dunque, denominati "essenziali" (o "*standard essential patents*").

Nella maggior parte dei casi, lo standard e il brevetto essenziale vengono introdotti e utilizzati nella produzione delle imprese aderenti prima della conclusione dei contratti di licenza sui brevetti. Le negoziazioni si tengono in un secondo momento, fuori dalle organizzazioni deputate a definire la standardizzazione tecnica[5].

Durante le successive negoziazioni, può accadere che imprese e titolari dei brevetti non raggiungano un accordo per la licenza. Il titolare, quindi, agisce in giudizio per far valere la contraffazione e ottenere l'esclusione dal mercato dei prodotti del contraffattore.

Il fallimento delle negoziazioni e la richiesta di un provvedimento inibitorio su un brevetto essenziale possono avere vari effetti.

"ICT" ("*Information and Communication Technology*"). Al riguardo si v. COMMISSIONE EUROPEA, *Patents and Standards: a modern framework for IPR-based standardization, final report*, 2014, disponibile su https://ec.europa.eu/growth/industry/intellectual-property/patents/standards_it. V. anche *Linee Direttrici sull'Applicabilità dell'Articolo 101,* cit., par. 308.

4 Per fare un esempio, nel caso dello standard "Long Term Evolution", coinvolto nella vicenda *Huawei,* i brevetti essenziali erano più di 4700; CORTE DI GIUSTIZIA, Causa C-170/13, *Huawei v. ZTE,* 16 luglio 2015, par. 40.

5 Le organizzazioni di standardizzazione, infatti, vietano che, nella stessa sede in cui si lavora alla definizione delle norme tecniche, si svolgano le negoziazioni. Si v., ad esempio, la politica dell'ETSI (l'organizzazione di standardizzazione attiva nel settore delle telecomunicazioni in Europa): v. ETSI, *Guide on Intellectual property rights*, 2013, punto 4.1. Le ragioni di questi divieti sono varie. Il timore che tali forme di negoziazione tra concorrenti possano essere oggetto di scrutinio antitrust, come intese restrittive della concorrenza, è una di queste. Un'altra ragione che spinge le organizzazioni a ritardare le negoziazioni sta nel fatto che coloro che concretamente prendono parte ai lavori sono per lo più esperti tecnici del settore e non rappresentanti commerciali dell'impresa. La trasformazione dell'organizzazione di standardizzazione in una sede di negoziazioni commerciali, poi, rallenterebbe notevolmente i lavori di definizione delle norme. Sul tema delle negoziazioni anticipate v. FARRELL – HAYES – SHAPIRO - SULLIVAN, 2007, 630 ss; CONTRERAS, 2013, 59 ss. Per una recente analisi sul tema dell'applicazione del divieto di intese alle regole statutarie sulla proprietà intellettuale delle organizzazioni si v. LO BUE, 2016, 537 ss. Per un'analisi degli impegni anticipati di prezzo da parte dei titolari di brevetti si v. LERNER - TIROLE, 2015, 547 ss.

Un primo effetto è quello c.d. di “esclusione”: l’utilizzatore, accusato di contraffazione, vede la propria produzione espulsa dal mercato e la creazione di una barriera all’entrata sullo stesso mercato.

Un secondo effetto possibile è quello c.d. di “sfruttamento”. L’utilizzatore, durante le negoziazioni, sarà disposto ad accettare condizioni molto svantaggiose, pur di non subire le conseguenze di “esclusione”. Pertanto, minacciando di agire in giudizio, il titolare del brevetto può imporre condizioni vessatorie sulla controparte.

3. Impegni FRAND. Tali effetti dell’azione del titolare possono determinare l’insuccesso dello standard e scoraggiare la futura partecipazione alle attività di standardizzazione. Una prima forma di reazione ai comportamenti dei titolari dei brevetti essenziali deriva, dunque, dalle stesse organizzazioni di standardizzazione.

Le organizzazioni impongono ai partecipanti, in primo luogo, di rivelare, durante i lavori, i brevetti detenuti che potrebbero riguardare lo standard in discussione. In secondo luogo, richiedono ai titolari di impegnarsi, fin dall’inizio dei lavori di standardizzazione, a concedere licenze a terzi a condizioni eque, ragionevoli e non discriminatorie (“*fair, reasonable and non discriminatory*”, da cui l’acronimo “FRAND”).

Il titolare del brevetto che, anziché concedere la licenza, attivi i rimedi inibitori viola gli impegni assunti in sede di standardizzazione. Il suo comportamento configura un inadempimento ad un obbligo assunto nei confronti delle organizzazioni o degli altri partecipanti (sul tema della natura giuridica dell’impegno FRAND v. LIBERTINI, 2013, 57 ss.; MAUGERI, 2014, 48 ss.; v. anche sul tema del rapporto tra l’interpretazione in chiave civilistica dell’impegno FRAND e i principi del diritto antitrust LIBERTINI, 2017, 16 ss.).

4. **Standrard e diritto della concorrenza.** Per altro verso, lo stesso comportamento chiama in causa le disposizioni antitrust[6].

Da una parte, infatti, il brevetto garantisce l'incentivo ad investire in attività di ricerca e di sviluppo, alimentando la spinta al progresso dinamico dei mercati. Ha, dunque, un effetto "pro-competitivo".

Dall'altra parte, tuttavia, l'impresa titolare di un brevetto essenziale allo standard può escludere i concorrenti dal mercato, causando una riduzione nella varietà dell'offerta sul mercato a valle; può imporre condizioni di licenza eccessivamente gravose e porre così le condizioni per un aumento dei prezzi sui consumatori finali; può innalzare barriere artificiali all'entrata dei mercati, il che impedisce l'introduzione di offerte innovative da parte dei concorrenti; infine, può trasferire la propria posizione di forza sul mercato a valle, proteggendosi dalla minaccia di entrata di concorrenti (sul tema degli effetti anticompetitivi dei provvedimenti inibitori v., fra molti, FARRELL - HAYES – SHAPIRO - SULLIVAN, 2007; LEMLEY - SHAPIRO, 2007, 1992 ss; non tutti gli autori sono, però, d'accordo nel ritenere che i comportamenti del titolare del brevetto essenziale siano sicuramente anticompetitivi. V., ad esempio, SIDAK, 2008, 715 ss; GERADIN - RATO, 2007, 128 ss; GUPTA, 2013, 827 ss).

Il dibattito sui brevetti essenziali si è dunque concentrato sull'individuazione delle condizioni in cui l'esercizio del brevetto trascende la tutela della proprietà industriale e si traduce in un pregiudizio alla concorrenza e ai consumatori, tale da giustificare un intervento antitrust (GHIDINI - FALCE, 2001, 315. TEECE - SHERRY, 2003, 1913; PARDOLESI - GRANIERI, 2004, 7; GRANIERI, 2004, 138; CALDERINI - GIANNACCARI - GRANIERI, 2005; DREXL, 2011, 210 ss. LIBERTINI, 2014, 176 ss. GHIDINI, 2015, 7. COLANGELO, 2016; v. anche DENOZZA, 2017, 20 ss. dove l'A. sostiene che nell'analizzare la questione degli standard

6 L'importanza antitrust dell'impegno FRAND emerge chiaramente dalle Linee Guida della Commissione, sopra citate. Si v., in particolare, i par. 283 e ss., dove si afferma che la presenza di una clausola FRAND è requisito essenziale affinché gli accordi di standardizzazione produttiva possano essere esentati dall'applicazione del divieto delle intese anticoncorrenziali. Essa risponde infatti all'esigenza di assicurare che gli accordi di standardizzazione siano aperti a tutti gli operatori del mercato. Quindi, la clausola FRAND è una delle condizioni in presenza delle quali l'accordo di standardizzazione rientra nel "*safe harbour*" delineato dalla Commissione nelle Linee Guida con riferimento all'articolo 101 TFUE.

dal punto di vista del diritto antitrust si debba anzitutto stabilire quale sia la categoria maggiormente meritevole di tutela tra quella dei consumatori che preferiscono meno innovazione e più concorrenza di prezzo e quella dei consumatori che, invece, preferiscono maggiore innovazione e meno concorrenza di prezzo).

5. **L'applicazione del diritto della concorrenza alle azioni inibitorie relative ai brevetti essenziali.** Parte della dottrina (CHAPPATTE, 2009, 331ss; CHAPPATTE, 2010, 175 ss. JONES, 2014, 1; in senso contrario, GERADIN - RATO, 2007, 101 ss e GERADIN - RATO, 2010, 129 ss; ritiene che il fenomeno debba essere affrontato attraverso un intervento di regolazione LIBERTINI, 2017, 9), la Commissione europea[7] e la giurisprudenza di vari Stati membri[8] sono concordi nell'affermare che la minaccia, la richiesta o l'esecuzione di un provvedimento inibitorio da parte di un titolare di brevetti essenziali può determinare l'applicazione del diritto della concorrenza.

Il dibattito che si è sviluppato su questo tema riguarda, soprattutto, le condizioni alle quali il ricorso al rimedio inibitorio possa costituire un abuso ai sensi dell'articolo 102 TFUE.

Secondo una prima tesi, in un contesto di standardizzazione, il ricorso all'inibitoria configurerebbe sempre un abuso se attuato dal titolare di un brevetto essenziale, una volta dimostrata la sua posizione dominante sul mercato.

---

7 COMMISSIONE EUROPEA, caso COMP/M.6381, *Google/Motorola Mobility,* 13 febbraio 2013, par. 107 ss; COMMISSIONE EUROPEA, caso AT.39939, *Samsung*, 29 aprile 2014; COMMISSIONE EUROPEA, caso AT.39985, *Motorola,* 29 aprile 2014.

8 Per la giurisprudenza italiana, v. TRIB. GENOVA, 8 maggio 2004, ord., in *Il Dir. Ind.*, 2005, 500, con nota di GRANIERI; TRIB. MILANO, 6 dicembre 2011 (dep. Il 5 gennaio 2012) ord., in *Giur. Italiana*, 2013, 86, con nota di VALENTE. Per la giurisprudenza tedesca e inglese v. infra nota 25 e 62. Per un'analisi della più rilevante giurisprudenza degli Stati membri si v. LAROUCHE - ZINGALES, 2014, 551. Per la giurisprudenza statunitense si v., ad esempio, *Apple Inc. v. Motorola Inc.* No. 1:11-cv-8540, opinioni e ordine del 22 giugno 2012, 18 ss. Si v. poi la decisione della FEDERAL TRADE COMMISSION, *In the matter of Motorola Mobility LLC and Google Inc.,* 24 luglio 2013, dkt. C-4410, FTC file n. 121-0120. Ancora, l'opinione della FTC rivolta all'ITC, *In re Certain Wireless Communication Devices, Portable Music & Data Processing Devices, Computers & Components Thereof*, Inv. No. 337-TA-745, 6 giugno 2012, 4 ss.

L'istituto del brevetto, in generale, attribuisce al titolare il diritto di uso esclusivo e il diritto ad ottenere un corrispettivo per l'utilizzo altrui dell'invenzione. In questo modo, si assicura all'inventore un adeguato premio-incentivo per l'innovazione raggiunta. Secondo alcuni[9], il titolare del brevetto, assumendo in seno all'organizzazione di standardizzazione un impegno FRAND, rivela che la diffusione dell'invenzione e il percepimento di un corrispettivo per l'utilizzo altrui costituiscono un ritorno adeguato per la propria attività innovativa. In altri termini, il diritto di utilizzare l'invenzione in via esclusiva non sarebbe indispensabile ad assicurargli incentivi ad innovare. Si conclude che, in caso di violazione del brevetto, il titolare ha diritto al solo risarcimento dei danni; non ad esercitare un'azione di contraffazione per escludere prodotti dal mercato. Il ricorso al rimedio inibitorio avrebbe, infatti, un effetto anti-competitivo non giustificato dalla necessità di premiare un'attività innovativa.

L'impegno FRAND è, dunque, interpretato come una "rinuncia al diritto" di impedire che altri si serva dell'invenzione brevettata, a condizione che il titolare ottenga un ritorno economico adeguato (tra gli autori che interpretano l'impegno FRAND come una rinuncia all'inibitoria in generale, v. MILLER, 2007, 374 ss.; LEMLEY, 2002, 1925 dove l'A. sostiene che l'impegno FRAND debba essere interpretato come una licenza tacita del brevetto, non lasciando spazio così a richieste inibitorie; LICHTMAN, 2010, 1042 ss.[10]).

Varie sono state le obiezioni a queste tesi. Secondo alcuni commenti, l'abbandono totale del rimedio inibitorio comporta un eccessivo sacrificio della

9 Si tratta dell'interpretazione data dal giudice Posner in *Apple v. Motorola,* 869 F. Supp. 2d 901 (N.D. Ill. 2012). Questi argomenti sono stati poi richiamati dalla Commissione europea per sostenere che il contesto della standardizzazione e l'impegno FRAND configurano "circostanze eccezionali" che giustificano una limitazione all'esercizio dei diritti di proprietà industriale: v. Decisione della Commissione, Caso AT.39939, *Samsung,* 29 aprile 2014, par. 61, dove la Commissione però non arriva a sostenere che la richiesta di provvedimenti inibitori su brevetti essenziali configuri sempre un abuso di posizione dominante.

10 Nello stesso senso anche la motivazione della decisione statunitense *Apple Inc. v. Motorola Inc.*, cit, 22 ss (il punto è stato criticato dalla successiva sentenza del Federal Circuit sulla stessa vicenda, *Apple v. Motorola,* 24 aprile 2014, 757 F. 3d 1286: in particolare, qui si afferma che non è opportuno costruire divieti *per se* in materia. La Commissione europea concorda su quest'ultimo punto: si v., ad esempio, la Decisione nel caso *Samsung,* cit., par. 55 ss.) V. anche FTC, *In re Certain Wireless,* cit, e FTC, *Statement In the matter of Google Inc.,* FTC file n. 121-0120, 3 gennaio 2013.

privativa industriale. Ai sensi della teoria della rinuncia, l'utilizzatore che violi il brevetto rischia solo di essere condannato a risarcire i danni. Generalmente, tali danni vengono quantificati in una somma simile al livello FRAND dei corrispettivi previsti nei contratti di licenza. All'utilizzatore allora converrebbe violare il brevetto, proponendo al titolare contratti a condizioni sub-FRAND, cioè inique "al ribasso". Il titolare del brevetto, per ottenere il pagamento FRAND, dovrebbe rivolgersi al giudice per il risarcimento dei danni. Allora, è probabile che, piuttosto che affrontare le lungaggini e le incertezze di un giudizio, preferisca accettare di stipulare il contratto a condizioni non convenienti.

Secondo queste opinioni, dunque, limitare del tutto il ricorso al rimedio inibitorio ha l'effetto di privare il titolare della privativa della remunerazione necessaria a premiare la sua attività inventiva. Inoltre, disincentiva le imprese innovative a prendere parte ai lavori di standardizzazione, generando un evidente ostacolo al progresso dinamico di un settore industriale (criticano la teoria della rinuncia con argomentazioni di questo tipo GERADIN - RATO, 2007., 119 ss. V. anche MARINIELLO, 2013, 5 ss. Si v. anche la *dissenting opinion* del giudice Rader in FED. CIRC. *Apple Inc. v. Motorola Inc.*, cit).

6. **Il confronto tra Commissione e Giudici nazionali.** Secondo le ultime considerazioni, le azioni inibitorie per i brevetti essenziali non possono essere considerate abusive di per sé ma solo a certe condizioni. Su quali siano queste condizioni vi è ampio dibattito.

Un primo ordine di idee, fondato su un approccio legato all'analisi economica del diritto, sostiene che il carattere abusivo dell'azione debba essere determinato tramite un bilanciamento di interessi nel caso concreto: se i costi sociali dell'esercizio del brevetto sulla collettività sono maggiori dell'incremento di ricompensa per il titolare del brevetto, l'azione inibitoria costituisce un abuso[11].

Secondo una parte della dottrina (PETIT, 2013, 677 ss.; TELYAS, 2014, 199 ss.), invece, l'inibitoria dovrebbe essere considerata abusiva solo se soddisfa il

11 Menziona quest'interpretazione TRIB. MILANO, 6 dicembre 2011, cit.

test elaborato dal Tribunale dell'Unione Europea in *ITT Promedia*[12] (per una ricostruzione delle conseguenze di questa tesi ZOGRAFOS, 2014, 53). In questa sentenza è stata elaborata una regola, da interpretare in senso restrittivo[13], per individuare i casi in cui l'esercizio di un'azione in giudizio costituisca illecito ai sensi dell'articolo 102 TFUE. In particolare, l'azione che non si può ragionevolmente considerare diretta a far valere i diritti dell'impresa interessata (e abbia, pertanto, unicamente natura defatigatoria) e che sia concepita nell'ambito di un piano volto ad eliminare la concorrenza è abusiva[14].

Le tesi decisamente prevalenti, però, sono quelle che considerano abusive le azioni inibitorie promosse nei confronti di un contraffattore dichiaratosi disposto a negoziare (c.d. *willing licensee*, su cui si v. ad esempio, DOLMANS, 2002, 163 ss; JONES, 2014, 24 ss)[15].

La soluzione del "*willing licensee*" pone il problema di determinare quando il contraffattore debba essere considerato disposto a stipulare un contratto di licenza a condizioni FRAND.

---

12 TRIBUNALE DELL'UNIONE EUROPEA, causa T-111/96, *ITT Promedia contro Commissione delle Comunità europee,* 17 luglio 1998, par. 60 ss; la regola è stata confermata da una recente decisione: TRIBUNALE DELL'UNIONE EUROPEA, causa T-119/09, *Protégé International contro Commissione europea,* 13 settembre 2012.

13 TRIBUNALE DELL'UNIONE EUROPEA*, ITT Promedia,* par. 61.

14 La Commissione europea e la Corte di Giustizia non sono d'accordo con la citata dottrina. La Commissione, infatti, nella decisione *Motorola* (caso AT.39985, *Motorola,* 29 aprile 2014, par. 531 ss.), ha espressamente rifiutato di applicare il test *ITT Promedia* alla materia dei brevetti essenziali. Secondo la Commissione, il test *ITT Promedia* non costituisce un precedente insuperabile e, comunque, il caso dei brevetti essenziali ad uno standard si distingue da quello che ha portato alla sentenza del Tribunale. Da parte sua, la Corte di Giustizia, nella sentenza *Huawei* non richiama la sentenza *ITT Promedia.* Per la tesi secondo cui l'atteggiamento della Commissione sarebbe comunque in linea con il precedente *ITT Promedia*, si v. TELYAS, 2014, 205 ss. V. anche PADILLA - O'DONOGHUE, 2013, 705, per una critica all'applicazione del test *ITT Promedia* al caso degli standard.

15 Si v. COMMISSIONE, caso COMP/M.6381, *Google Motorola Mobility,* 13 febbraio 2012; v. il comunicato stampa (disponibile sul sito www.europa.eu) e la decisione (caso AT.39939, *Samsung*, cit.) della Commissione europea nel caso *Samsung*. Samsung aveva richiesto l'inibitoria per alcuni brevetti essenziali, in risposta ad alcune azioni di Apple portate avanti negli Stati Uniti (v. *Apple, Inc. v. Samsung Electronics Co., Ltd*., No. 5:11-cv-01846, N.D. Cal. Apr. 15, 2011). La Commissione ha aperto un'indagine sul comportamento di Samsung. La vicenda si è chiusa nel 2014 con l'accettazione da parte della Commissione degli impegni proposti da Samsung. Ancora, si v. la decisione della COMMISSIONE EUROPEA, caso AT.39985, *Motorola,* 29 aprile 2014. Concorde nel ritenere che le inibitorie siano vietate se portate avanti contro *willing licensees* è la Federal Trade Commission statunitense: v. FTC, *In the matter of Motorola Mobility LLC and Google Inc.,* 24 luglio 2013, dkt. C-4410, FTC file n. 121-0120 (anche se la FTC non ha richiamato, nella decisione, lo Sherman Act ma il FTC Act, sezione 5). Ancora, si v. Fed. Circ. *Apple Inc. v. Motorola Inc.*, cit.

Secondo una prima lettura, fatta propria dalla Commissione europea[16], l'utilizzatore che dichiara di vincolarsi alla definizione di "FRAND *terms*" data da un giudice o da un terzo arbitratore è senz'altro "*willing*"[17]. In mancanza di tale dichiarazione, la disponibilità a negoziare deve essere valutata "caso per caso". Nell'interpretazione della Commissione, dunque, basta una dichiarazione dell'utilizzatore perché l'inibitoria del titolare possa essere qualificata come un abuso, ai sensi dell'articolo 102 TFUE[18].

Sensibilmente diversa l'interpretazione di "*willing licensee"* offerta dalla giurisprudenza tedesca[19]. In particolare, l'utilizzatore dello standard sarebbe "*willing"* solo nel caso in cui abbia presentato al titolare del brevetto una proposta incondizionata che il titolare non può rifiutare senza ostacolare in modo iniquo il contraffattore o senza violare il principio di non discriminazione[20]. Inoltre, quando utilizza l'invenzione brevettata prima dell'accettazione di una tale proposta da parte del titolare, il contraffattore deve osservare gli obblighi che sarà tenuto a rispettare sulla base del futuro contratto di licenza; in

16 COMMISSIONE EUROPEA, decisione nel caso AT.39985 *Motorola*, cit, par 437.

17 Secondo la Commissione, inoltre, non è necessariamente "*unwilling*" l'utilizzatore che contesta la validità, la contraffazione o il carattere essenziale del brevetto; invece, è da considerare generalmente "*unwilling*" l'utilizzatore che non risponde alle proposte del titolare o pone in essere tattiche dilatorie (si v. MEMO/14/322, *Antitrust Decisions on Standard Essential Patents - Motorola Mobility and Samsung- Frequently Asked Questions,* 29 aprile 2014).

18 La Commissione è stata criticata perché non chiarisce in che momento l'utilizzatore debba fare la dichiarazione per poter essere considerato senz'altro "*willing*"*.* Il rischio è che l'utilizzatore possa ritardare le negoziazioni e effettuare la dichiarazione solo nel momento in cui il titolare esercita l'inibitoria, in modo tale da bloccarla. In quest'ipotesi, il risultato sarebbe quello temuto dai critici della teoria della rinuncia: l'inibitoria diventa un rimedio inesistente; il titolare si trova di fronte all'alternativa fra iniziare un procedimento per ottenere il risarcimento dei danni o stipulare immediatamente una licenza *sub*-FRAND. Sul punto TELYAS, 2014. 211. In realtà, è più probabile che la Commissione abbia inteso escludere l'applicazione della regola nel caso in cui l'utilizzatore non risponda alle proposte o ritardi le negoziazioni: ha infatti, affermato, che questi ultimi comportamenti sono generalmente indici di "*unwillingness*".

19 La giurisprudenza richiamata trova origine dalla decisione della BGH, *Orange Book*, KZR 39/06, 6 maggio 2009.

20 La giurisprudenza tedesca, successiva alla pronuncia *Orange Book,* ha affermato che, affinché la proposta del licenziatario sia "incondizionata e irrevocabile" quest'ultimo deve rinunciare a contestare la validità, il carattere essenziale o la contraffazione del brevetto (LANDGERICHT MANNHEIM, causa *GPRS-Zwangslizenz*, 7 O 122/11, 9 dicembre 2011). Come anticipato, la Commissione ha assunto posizione opposte al riguardo: casi COMP/93.939 e COMP/39.985, MEMO/14/322, 29 aprile 2014. La posizione della Commissione è stata confermata dalla Corte di Giustizia nella sentenza *Huawei* (par. 69).

particolare rendere conto degli atti di sfruttamento e pagare i relativi corrispettivi[21].

Quindi, per la giurisprudenza tedesca, l'inibitoria è un abuso esclusivamente nel caso in cui l'aspirante licenziatario abbia preso l'iniziativa delle negoziazioni e abbia tenuto una serie di comportamenti attivi. Nell'interpretazione della Commissione, invece, si ha abuso anche se il licenziatario, pur non tenendo comportamenti attivi, sia manifestamente disposto a negoziare nel caso concreto.

Il contrasto interpretativo tra giurisprudenza tedesca e decisioni della Commissione ha spinto il Landgericht Düsseldorf al rinvio di cinque questioni pregiudiziali alla Corte di Giustizia nella vicenda *Huawei*[22]. Con le questioni pregiudiziali, il giudice ha chiesto, in sostanza, a quali condizioni l'azione inibitoria per un brevetto essenziale sia contraria all'articolo 102 TFUE.

7. La sentenza Huawei: prima parte. Nella sentenza della Corte si possono distinguere due parti. Nella prima parte[23], la Corte pare elaborare una regola generale in materia di inibitorie su brevetti essenziali ad uno standard. Nella seconda, elabora una regola più specifica, basata su una procedura di negoziazione che il titolare del brevetto e l'utilizzatore devono rispettare[24].

Per ciò che riguarda la prima parte della decisione, in particolare, la Corte afferma che, di fronte alla richiesta di inibitoria del titolare, l'utilizzatore può invocare l'articolo 102 se vi è stato, da parte del titolare, un rifiuto abusivo

21 Secondo la giurisprudenza tedesca, l'onere di provare la sussistenza di queste due condizioni ricade sul licenziatario, non sul titolare.

22 In particolare, le richieste alla Corte di Giustizia possono essere riassunte in questi termini: a) se, affinché l'azione sia abusiva, sia sufficiente la manifestazione di disponibilità a negoziare del contraffattore oppure sia necessaria una proposta vincolante e l'adempimento delle obbligazioni derivanti dalla ipotetica licenza; b) nel primo caso, a quali condizioni dovrebbe essere espressa tale disponibilità; c) nel secondo caso, a quali condizioni dovrebbe essere espressa la proposta vincolante; d) nel caso in cui si richieda l'adempimento delle obbligazioni derivanti dall'ipotetica licenza, a quali condizioni esso debba essere effettuato, se si debbano rivelare anche precedenti contraffazioni del brevetto e se possa bastare una garanzia dell'adempimento; e) se per le precedenti contraffazioni del brevetto sia sufficiente offrire le *royalties* ovvero si debbano risarcire i danni. CORTE DI GIUSTIZIA, causa C-170/13, *Huawei,* 16 luglio 2015, par. 39.

23 CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 48-54.

24 CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 55 ss.

di stipulare il contratto di licenza a condizioni FRAND.

Nell'indicare le circostanze in presenza delle quali il rifiuto del titolare del brevetto essenziale assume carattere abusivo, la decisione non coincide con l'orientamento generale della giurisprudenza in materia di rifiuto di licenza su un diritto di proprietà intellettuale. Secondo tale orientamento generale, come noto, in presenza di alcune circostanze eccezionali il rifiuto di concedere accesso ad un diritto di proprietà intellettuale può costituire violazione dell'articolo 102 TFUE. Le circostanze eccezionali elaborate dalla giurisprudenza sono il risultato di un bilanciamento tra l'interesse a garantire un adeguato premio-incentivo all'attività innovativa del titolare e l'interesse ad evitare effetti anticoncorrenziali sul mercato. In particolare, la giurisprudenza riscontra un abuso ai sensi dell'articolo 102 se: 1) il diritto di proprietà intellettuale è indispensabile per una certa attività su un mercato secondario; 2) vi è un netto rifiuto di stipulare una licenza da parte del titolare oppure la richiesta di condizioni talmente gravose da costituire di fatto un rifiuto; 3) il rifiuto di concedere licenza su tale diritto impedisce l'emergere di un prodotto nuovo o limita lo sviluppo tecnologico in altro modo a danno dei consumatori; 4) il rifiuto non è oggettivamente giustificato; 5) vi è il rischio che qualsiasi concorrenza effettiva sul mercato secondario risulti eliminata[25].

A differenza della consolidata regola giurisprudenziale, nel caso di rifiuto di licenza su brevetti essenziali ad uno standard la Corte pone una regola speciale. Essa ravvisa nel carattere essenziale del brevetto e nell'esistenza di un impegno FRAND assunto dal titolare due circostanze eccezionali, in virtù delle quali il titolare è in grado di controllare l'accesso altrui ad una norma tecnica e, quindi, di sfruttare le legittime aspettative che il proprio impegno FRAND crea negli aderenti. Infatti, l'impegno FRAND influisce sulla definizione tecnica dello standard e crea una situazione di dipendenza delle altre imprese

25 V. CORTE DI GIUSTIZIA, cause riunite C-241/91P e C-242/91P, *RTE e ITP v. Commissione*, 6 aprile 1995; CORTE DI GIUSTIZIA, causa C-418/01, *IMS Health v. NDC Health,* 29 aprile 2004 e TRIBUNALE DELL'UNIONE EUROPEA, causa T-201/04, *Microsoft Corp. v. Commissione,* 17 settembre 2007.

dal brevetto essenziale[26].

In considerazione di queste peculiarità, la Corte afferma che, nel caso degli accordi di standardizzazione, si ha abuso se: 1) il brevetto del titolare è essenziale per l'applicazione della norma tecnica; 2) vi è un previo irrevocabile impegno FRAND; 3) il titolare rifiuta di concludere un contratto a condizioni FRAND. Quest'ultima condizione comprende, in primo luogo, il caso in cui il titolare rifiuti di stipulare qualunque contratto e il caso in cui proponga condizioni contrattuali talmente vessatorie da costituire un rifiuto di fatto (sono ipotesi in cui il titolare del brevetto intende ottenere un effetto di "esclusione"). Allo stesso tempo, la condizione sub 3), appena richiamata, comprende l'ulteriore situazione in cui il titolare del brevetto imponga delle condizioni tali da non costituire un rifiuto di fatto, ma tali da garantirgli il percepimento di sovraprofitti monopolistici; anche l'imposizione di condizioni vessatorie ed eccessive configura, infatti, un rifiuto di stipulare un contratto ragionevole. La regola della Corte si applica perciò sia ai casi in cui l'azione inibitoria configuri un abuso "escludente" sia al caso in cui essa costituisca lo strumento per attuare una strategia abusiva di "sfruttamento" del potere di mercato[27]. La regola posta dalla Corte ha dunque un ambito di applicazione molto ampio. In

26 CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 48 ss. La Corte si trova d'accordo con l'Avv. Gen. Whatelet sul punto (Conclusioni dell'Avv. Gen. Whatelet, cit. par. 70). Sulla distinzione tra la sentenza *Huawei* e la precedente giurisprudenza europea v. OSTI, 2017, 4 e ss.

27 Il punto è rilevante perché, secondo alcuni autori, le regole elaborate dalla Corte nella decisione *Huawei* riguardano solo il caso in cui il titolare sia interessato a dominare il mercato a valle (abuso "escludente"); non invece il caso in cui il titolare, assente nel mercato a valle dei prodotti, intenda solamente sfruttare il suo brevetto essenziale per ottenere profitti eccessivi. Tali autori fanno leva sul fatto che la Corte non tratta il tema dei profitti monopolistici nella motivazione e si concentra solo sugli effetti di "esclusione" dei concorrenti dal mercato. V. PETIT, 2017. V. anche BRANKIN - CISNAL DE UGUARTE - KIMMEL, 2016, 520; cfr. RATO, ENGLISH, 2016, 110; MUSCOLO, 2017, 17.
Tuttavia, la regola che la Corte elabora finisce per includere nel suo ambito anche il mero "sfruttamento" del proprio potere di mercato da parte del titolare del brevetto. Inoltre, se è vero che la Corte fa espressamente riferimento solo all'effetto "escludente" dell'inibitoria, nel ricostruire gli effetti anticoncorrenziali del rifiuto di accesso ad un brevetto essenziale, tratta anche delle "legittime aspettative" create dal previo impegno FRAND del titolare. Quest'ultimo punto si traduce, a mio avviso, in un implicito richiamo al tema dello "sfruttamento" abusivo da parte del titolare del brevetto della situazione di debolezza contrattuale delle controparti. Sul tema dell'applicazione delle regole elaborate dalla Corte anche al caso delle imprese non verticalmente integrate v. COLANGELO, 2016, 275 ss; LUNDQVIST, 2015, 391. Interpreta la sentenza nel senso che si applichi anche ai titolari di brevetti non presenti nel mercato a valle GERADIN, 2016. V. anche LANDGERICHT DÜSSELDORF, 4a O 73/14, 4a O126/14, 4a O 127/14, 4a O 128/14, 4a O 129/14, 4a O 130/14, 31 marzo 2016, *Saint Lawrence v. Vodafone.*

particolare, l'applicazione dell'articolo 102 viene a coprire la gran parte dei casi di uso scorretto degli strumenti di *enforcement* da parte dei titolari dei brevetti in posizione dominante, andando così a sovrapporre l'abuso di posizione dominante alla più generale figura dell'abuso delle inibitorie da parte del titolare dei brevetti[28].

8. Il rapporto con la giurisprudenza precedente. Le circostanze eccezionali su cui la Corte fonda la regola appena descritta in materia di brevetti essenziali rivelano un approccio della Corte molto diverso da quello finora impiegato per l'analisi di rifiuto di licenza di diritti di proprietà intellettuale (nel senso che la presenza di tali circostanze eccezionali siano sufficienti a ritenere abusivo un successivo rifiuto v. JONES, 2014, 25 ss; di opinione contraria, VESTERDORF, 2013, 109 ss.).

In primo luogo, la regola elaborata nella decisione in commento prescinde da una qualunque analisi degli effetti anticoncorrenziali sul mercato a valle e dell'impedimento allo sviluppo tecnico dell'industria. In presenza di impegni FRAND su brevetti essenziali, la Corte sembra dare tali effetti per scontati.

La regola riguarda, poi, non solo i casi in cui l'esercizio del brevetto determini l'esclusione dei concorrenti; ma anche i casi in cui la minaccia di tale effetto "escludente" configuri lo strumento per sfruttare il proprio potere di mercato, con riferimento, peraltro, ad un settore, come quello della proprietà industriale, dove i sovraprofitti del titolare dovrebbero costituire parte della sostanza stessa della privativa.

L'approccio innovativo della Corte in materia di standard si giustifica per alcune peculiarità della standardizzazione rispetto ai casi di esercizio di una qualunque privativa intellettuale.

In primo luogo, negli standard l'esistenza di un impegno FRAND offre

28 L'esercizio strategico dell'azione inibitoria da parte del titolare di un brevetto essenziale che non ricopra una posizione dominante sul mercato, pur non violando l'articolo 102, potrebbe comunque essere ritenuto contrario alla clausola di buona fede o al principio del divieto di abuso del diritto di brevetto (PICHT, 2016, 371).

un'indicazione rilevante sugli incentivi del titolare del brevetto. La promessa del titolare rivela che il ritorno economico derivante dalla stipulazione di licenze è considerato sufficiente dal titolare per premiare gli investimenti effettuati e l'attività innovativa portata avanti, anche alla luce dell'accrescimento delle utilità potenziali connesse con il fatto che il brevetto può essere diffuso in un contesto più ampio. Di conseguenza, l'impegno FRAND mostra che il mantenimento dell'esclusiva sul brevetto in capo al titolare non è essenziale affinché egli possa ritenersi premiato per l'attività innovativa. In presenza di questo impegno, aumenta la probabilità che il successivo rifiuto di stipulare una licenza nasconda una pratica anticoncorrenziale persecutoria nei confronti dei concorrenti, anziché una misura volta a tutelare gli incentivi del titolare del brevetto[29]. L'esistenza di un impegno FRAND assunto dal titolare del brevetto è rilevante, quindi, per l'operazione di bilanciamento tra l'interesse a garantire un adeguato premio-incentivo all'attività innovativa e l'interesse al funzionamento concorrenziale del mercato.

In secondo luogo, la regola giurisprudenziale "tradizionale" sul rifiuto di licenza applica l'articolo 102 a condizione che vi sia l'eliminazione della concorrenza effettiva sul mercato a valle. Negli standard, anche i comportamenti che non hanno l'effetto di eliminare ogni concorrenza a valle possono generare un pericoloso ostacolo al progresso tecnico. L'effetto di efficienza dinamica generato dallo standard dipende dalla sua diffusione e dall'estensione della rete che esso stesso crea. L'eliminazione dal mercato di un utilizzatore riduce l'intercomunicabilità nel sistema e potrebbe determinare l'insuccesso dello standard. Il rifiuto di licenza negli standard merita dunque un approccio diverso rispetto a quello classico in materia.

9. Standard "de iure" e standard di fatto. Il discorso è peraltro parzialmente diverso se si confrontano gli standard "*de iure*" (quelli elaborati nelle organizzazioni di standardizzazione e interessati da impegni FRAND) e gli

29 Resta ferma la possibilità per il titolare di agire in giudizio per la presentazione dei dati contabili relativi agli atti di sfruttamento o per il risarcimento del danno subito (CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 76).

standard c.d. “di fatto”. Questi ultimi sono standard che emergono dal mercato, non dalla decisione di un’organizzazione di imprese, e possono consistere in una soluzione tecnica coperta da un brevetto. Gli standard di fatto non rientrano nell’applicazione della regola elaborata dalla Corte nella decisione in commento, in quanto manca un impegno FRAND. Eppure, tra standard di fatto e standard *de iure* esistono alcune caratteristiche simili che avrebbero forse giustificato l’applicazione delle stesse regole.

Negli standard di fatto non esiste l’impegno FRAND e, dunque, manca quell’indicazione per cui il ritorno economico derivante dalle licenze rappresenta premio sufficiente per l’attività inventiva del titolare. Tuttavia, un’indicazione indiretta in tal senso è offerta dallo stesso fatto che l’invenzione oggetto del brevetto abbia avuto una diffusione tale da diventare standard del mercato. Infatti, anziché sfruttare in esclusiva il brevetto, il titolare ha concesso l’accesso alla propria tecnologia a gran parte degli operatori industriali, dimostrando che l’ampia diffusione del brevetto a fronte di un ritorno economico costituisce un adeguato premio per l’attività innovativa intrapresa. Il successo dello standard sul mercato rappresenta, dunque, un’indicazione sugli incentivi del titolare simile a quella costituita dall’assunzione di un impegno FRAND. Pertanto, anche l’esistenza di uno standard di fatto dovrebbe essere tenuta in considerazione nel bilanciamento tra l’interesse a incentivare l’attività di ricerca innovativa e l’interesse alla tutela della concorrenza. Inoltre, anche nel caso in cui l’interconnessione dei prodotti su un mercato si basi su uno standard di fatto, l’esclusione di un solo partecipante dalla rete rappresenta un potenziale ostacolo allo sviluppo dinamico dell’industria.

Dunque, se è corretto distinguere le condizioni dell’intervento antitrust in materia di standard da quelle generali in materia di diritti di proprietà intellettuale, non appare altrettanto corretta l’adozione di un approccio completamente diverso tra standard *de iure* e standard di fatto (interpretano la sentenza, in parte, nel senso di elaborare regole comuni agli standard di fatto e *de iure* MAUME, 2016, 224, KORBER, 2016, 1119; sul tema della differenza di disciplina tra standard *de iure* e di fatto v. MELI, 2014; JACOBS - HÜBENER, 2016,

33 ss.; PICHT, 2016, 371 ss.).

10. La sentenza Huawei: seconda parte. La sentenza della Corte non si limita ad affermare che il carattere abusivo dell'inibitoria (e quindi l'applicazione dell'articolo 102) dipende dall'esistenza di un rifiuto abusivo di stipulare un contratto di licenza a condizioni FRAND. Infatti, nella seconda parte della decisione, viene elaborata una seconda regola. In particolare, la Corte qui stabilisce taluni presupposti in presenza dei quali il titolare del brevetto essenziale che agisce per l'inibitoria non abusa della propria posizione dominante[30].

L'abuso è da escludere, secondo la Corte, laddove: a) il titolare avverte l'utilizzatore dell'avvenuta contraffazione, prima di esperire l'azione[31]; b) il titolare effettua, nei contatti per addivenire all'accordo, una proposta di licenza "concreta e scritta" a condizioni FRAND, una volta che l'utilizzatore abbia comunicato di essere disposto a stipulare un contratto a condizioni FRAND[32]; c) il contraffattore non dà seguito a tale proposta con diligenza[33]; oppure effettua una controproposta non FRAND; d) l'utilizzatore non costituisce una garanzia appropriata[34], una volta che abbia effettuato una controproposta FRAND[35]e

30 CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 55 ss.

31 Nell'effettuare tale comunicazione deve anche specificare il brevetto violato e il modo in cui è avvenuta la contraffazione (CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 61). Le ragioni di questa comunicazione stanno nel fatto che spesso l'utilizzatore è ignaro dell'esistenza del brevetto essenziale (Conclusioni dell'Avv. Gen. Whatelet, in causa C-170/13, *Huawei,* 20 novembre 2014, par. 81).

32 La proposta deve essere effettuata per iscritto e deve indicare il corrispettivo e le sue modalità di calcolo. Il motivo per cui tocca al titolare del brevetto, anziché al contraffattore, presentare la prima proposta FRAND sta, secondo la Corte, nel fatto che l'esistenza di un impegno FRAND rende ragionevole tale soluzione. Inoltre, il titolare è nella migliore posizione per individuare condizioni non discriminatorie (CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 64).

33 In particolare, l'espressione "con diligenza" viene interpretata dalla Corte nel senso che il contraffattore debba dare risposta alla proposta rispettando "gli usi commerciali riconosciuti in materia" e comportandosi in buona fede. Il punto deve essere accertato sulla base di elementi obiettivi ed implica l'assenza di ogni tattica dilatoria (CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 65).

34 Tale garanzia dovrebbe essere costituita conformemente agli usi commerciali riconosciuti in materia, ad esempio fornendo una garanzia bancaria oppure consegnando le somme necessarie. Il calcolo di tale garanzia deve comprendere, in particolare, il numero dei precedenti atti di sfruttamento del brevetto di cui il contraffattore deve poter produrre un rendiconto (CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 67).

questa sia stata rifiutata dal titolare[36].

Il ricorrere delle condizioni esclude la responsabilità antitrust del titolare. A tal riguardo, una prima questione riguarda il rapporto logico tra l'affermazione contenuta nella prima parte della decisione (abusa il titolare che, dopo aver assunto nell'organizzazione di standardizzazione un impegno FRAND, rifiuti di stipulare un contratto di licenza a condizioni FRAND) e quella contenuta nella seconda parte (non abusa il titolare che, prima di proporre azione inibitoria, abbia rispettato la procedura di negoziazione delineata dalla Corte). Deve domandarsi infatti se tra la situazione certa di abuso (prima parte della decisione) e la situazione certa di non abuso (seconda parte) vi sia uno spazio per situazioni che, pur non soddisfacendo il test posto dalla decisione nella sua seconda parte, nondimeno debbano essere considerate lecite e non abusive. In altre parole, l'esclusione della responsabilità antitrust del titolare si ha soltanto se ricorrono le condizioni poste dalla Corte nella seconda parte della decisione (leggendo cioè l'espressione "non abusa laddove", usata dalla Corte, come "non abusa solo laddove") (BARTHELMESS – DOLMANS - ZIMBRON, 2015, 12) [37]? Oppure, in assenza di quelle condizioni, un'esclusione di responsabilità potrebbe comunque aversi in base alle circostanze del caso concreto (la regola

35 La controproposta FRAND deve essere effettuata entro un breve termine e per iscritto (CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 66).

36 Inoltre, la Corte afferma che, in seguito alla controproposta del contraffattore, se non si raggiunge un accordo sulle condizioni FRAND le parti possono rivolgersi ad un terzo indipendente che statuisca in termini brevi (CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 68). Infine, la Corte concorda con la Commissione europea (v. *supra* nota 26) sul fatto che l'utilizzatore del brevetto possa contestare, parallelamente alle negoziazioni relative alla concessione delle licenze, la validità di tali brevetti e il loro carattere essenziale (CORTE DI GIUSTIZIA, causa *Huawei,* cit., par. 69).

37 Alcune espressioni nel testo della decisione si pongono a sostegno di questa tesi. Ad esempio, con riferimento alla condizione sub a), la Corte afferma che «*a meno di violare l'articolo 102 TFUE, il titolare di un BEN che ritenga che quest'ultimo sia oggetto di contraffazione non può esperire, senza preavviso né consultazione preliminare del presunto contraffattore, un'azione inibitoria o per il richiamo di prodotti avverso quest'ultimo, neanche qualora il suddetto BEN sia già stato sfruttato dal presunto contraffattore*». Inoltre, la Corte, in più di un'occasione, si serve di espressioni che sembrano costruire i comportamenti delle parti come adempimento di veri e propri obblighi di comportamento: per esempio, si legge che «[l'impegno FRAND] *giustifica comunque che al medesimo sia imposto il rispetto di requisiti specifici all'atto della proposizione di azioni inibitorie o per il richiamo di prodotti avverso presunti contraffattori*». Ancora, «*spetta al suddetto titolare trasmettere a tale contraffattore una proposta di licenza concreta e scritta a condizioni FRAND*». Infine, l'avvocato generale, nelle sue conclusioni sul caso in questione, si era espresso per questa interpretazione: v. Conclusioni dell'Avv. Gen. Wathelet, causa C-170/13, 20 novembre 2014, par. 83 e 103.

della Corte configurando allora nulla più che un c.d. "*safe harbour*" per il titolare del brevetto) (RATO - ENGLISH, 2016, 103)?

Tra le due interpretazioni, la Corte sembrerebbe orientata in favore della seconda[38] e tale atteggiamento è da condividere. Non può dimenticarsi che per le ragioni dette, in un contesto di standardizzazione, il discrimine generale tra comportamento abusivo e non abusivo è il rifiuto del titolare del brevetto di concedere la licenza a condizioni FRAND (prima parte della decisione). E' certamente vero che tale rifiuto non si configura quando il titolare abbia tenuto un comportamento attivo offrendo di stipulare alle condizioni poste nella seconda parte della decisione. Tuttavia, non può escludersi che, in base alle circostanze del caso concreto, pur non avendo egli stesso assunto un'iniziativa formale, consti la sua disponibilità a stipulare, ad esempio, da fatti concludenti, come il sedere ad un tavolo di negoziazione e tenere comportamenti corretti e di buona fede; ovvero consti una indisponibilità di segno contrario, ad esempio, quando egli abbia invitato alle trattative il contraffattore con una proposta di apertura non FRAND senza riceverne risposta[39]. Non è difficile ipotizzare, del resto, che nel caso degli standard di fatto sia piuttosto questo criterio che non quello del "*safe harbour"* a trovare maggiore possibilità di applicazione in concreto, difettando tra il titolare e l'utilizzatore l'impegno FRAND o un altro

38 Si legge infatti che «*L'articolo 102 TFUE deve essere interpretato nel senso che il titolare di un brevetto essenziale (…), che si sia irrevocabilmente impegnato nei confronti di tale organismo a concedere a terzi una licenza a condizioni (…) «FRAND», non abusa della sua posizione dominante ai sensi di tale articolo quando…*». In tal senso può essere letto anche il paragrafo introduttivo del discorso (par. 55): «*al fine di evitare che un'azione inibitoria o per il richiamo di prodotti possa essere considerata abusiva, il titolare di un BEN deve rispettare taluni requisiti volti a garantire un giusto equilibrio degli interessi in gioco*». E' significativo che la Corte usi l'espressione "*possa essere considerata abusiva*" e non "*sia abusiva*". Sicuramente vi è una certa confusione nel modo di esprimersi della Corte: si v. al riguardo il par. 60 dove la Corte utilizza, invece, l'espressione "*a meno di non violare l'articolo 102*". L'interpretazione indicata nel testo è stata adottata anche nella decisione inglese HIGH COURT OF JUSTICE, *Unwired Planet v. Huawei,* 5 aprile 2017, par. 741.

39 Il fatto che le prime proposte del titolare non siano FRAND, infatti, non necessariamente comporta un rifiuto di stipulare un contratto a condizioni FRAND. E' normale, nella prassi degli scambi commerciali, che le prime proposte vengano effettuate a prezzi più elevati di quelli che ci si aspetta di ottenere alla fine delle contrattazioni. Certamente le proposte non FRAND del titolare costituiscono un rifiuto abusivo laddove l'utilizzatore abbia risposto sottolineando il carattere non FRAND delle proposte. Al contrario, se il contraffattore non offre alcuna risposta alle proposte il rifiuto pare potersi ravvisare più nel comportamento del contraffattore che non nelle proposte del titolare.

vincolo, contrattuale o precontrattuale, tra le due parti.

Tale convincimento appare rafforzato da un'ulteriore considerazione. Infatti, la prima interpretazione della sentenza farebbe dipendere l'applicazione dell'articolo 102 principalmente dall'accertamento del carattere FRAND delle proposte del titolare. Il limite di questo approccio sta nel fatto che non vi è certezza sul significato dell'espressione FRAND e la Corte non ha preso alcuna posizione sul punto. Sicché è forte il rischio che la prima interpretazione della decisione porti a risultati di arbitrarietà e incertezza nella soluzione delle controversie[40]. Pare allora più opportuno intendere la regola elaborata dalla Corte come un "*safe harbour"* (concorda con questa lettura della sentenza LIBERTINI, 2017, 12; ma l'A. afferma che la sentenza deve comunque essere interpretata nel senso di porre una presunzione di abuso e di offrire una forma di supplenza alla mancanza di regolazione in materia di *standard essential patents;* regolazione che, secondo l'A., avrebbe potuto essere realizzata attraverso una forma di gestione accentrata dei diritti di proprietà intellettuale. V. anche sul punto OSTI, 2017, 8).

Laddove le circostanze del caso concreto non ricadano nel "*safe harbour*", si tratterà di accertare se il comportamento tenuto dal titolare possa dirsi abusivo nel caso concreto. A tal fine, occorre tornare al principio elaborato

40 Questa incertezza pare riversarsi principalmente a danno della posizione del titolare del brevetto. Secondo la prima interpretazione della sentenza, infatti, l'azione inibitoria sarebbe sempre abusiva quando le proposte del titolare non siano FRAND. A tal fine, non avrebbe rilievo il fatto che il contraffattore non abbia dato alcuna risposta alle proposte del titolare e che sia questo il motivo per cui le trattative non sono andate avanti. Dunque, dato che il titolare difficilmente ha la certezza di aver proposto condizioni FRAND, egli è disincentivato ad agire in giudizio anche di fronte ad un comportamento scorretto della controparte. Il rischio per il titolare è infatti alto: se le proposte superano il livello FRAND la sua successiva azione costituirà comportamento abusivo. La controparte, invece, non corre lo stesso rischio, sicché probabilmente forzerà le negoziazioni verso una stipulazione a condizioni a sé favorevoli e, magari, sub-FRAND. Ciò potrebbe spingere il titolare del brevetto ad assumere un atteggiamento prudente nelle negoziazioni, abbassando il livello delle proprie proposte iniziali. Quindi, l'interpretazione qui criticata non solo potrebbe portare a sanzionare, *ex post*, fattispecie che non necessariamente pongono problemi antitrust; ma potrebbe anche avere l'effetto, *ex ante*, di privare di efficacia la tutela della proprietà intellettuale nel caso degli standard. V. sul tema PADILLA - O'DONOGHUE, 2013, 706. PICHT, 2016, 374. Si noti che l'Avv. Gen. nelle sue conclusioni aveva dato pari rilievo al comportamento del titolare e del contraffattore durante le trattative (Conclusioni, causa C-170/13, cit., par.80). V. anche LIBERTINI, *Brevi riflessioni sulla sentenza* Huawei, cit., dove l'A. sostiene che gli obblighi dell'utilizzatore debbano essere incondizionati. Sul tema dell'incertezza sul significato di FRAND si tornerà *infra.*

dalla Corte nella parte iniziale della sentenza per individuare l'abuso di posizione dominante in materia di standard. Pertanto, si dovrà stabilire se vi sia stato un rifiuto di stipulare un contratto di licenza a condizioni FRAND da parte del titolare di un brevetto essenziale che abbia assunto un impegno FRAND.

11. Hawuei e il rifiuto di concedere licenza. Il confronto tra la prima e la seconda parte della decisione evidenzia una differenza nel modo di esprimersi della Corte.

Laddove costruisce il "*safe harbour*", la Corte parla di carattere abusivo dell'inibitoria[41]. Invece, nella parte in cui elabora la regola generale, parla di carattere abusivo del rifiuto e, in via derivata, dell'inibitoria[42]. In altre parole, da una parte, sembra collegare la violazione dell'articolo 102 TFUE all'esercizio abusivo degli strumenti di *enforcement* e, dall'altra, al rifiuto abusivo di licenza.

La differenza di approccio è solo apparente. Il "*safe harbour*" consiste nel negare il carattere abusivo dell'azione in presenza di condizioni che dimostrano la genuina intenzione del titolare di concludere la licenza; di condizioni che dimostrano, quindi, la mancanza di un rifiuto. Anche laddove si parla di carattere abusivo diretto dell'azione, dunque, la "non abusività" dell'inibitoria è derivata dal "non rifiuto" del titolare.

L'incoerenza espressiva, però, non è irrilevante. La Corte costruisce una forma di "abusività derivata" dell'inibitoria. In altri termini, non pare attribuire il carattere abusivo all'inibitoria "in sé" (in senso contrario, però, BARTHELMESS – DOLMANS - ZIMBRON, 2015, 15. Argomenti a sostegno della tesi qui presentata si trovano in RATO - ENGLISH, 2016, 107). Piuttosto, lo fa dipendere dalla presenza di un rifiuto illecito. Ed è di questo rifiuto illecito che si occupa la sentenza: con il "*safe harbour*" si individua un caso in cui non c'è rifiuto; con la regola generale si individuano le circostanze in cui si ha illiceità del rifiuto. La sentenza pone dunque regole sul rifiuto di licenza, più che sull'esercizio abusivo dell'azione in giudizio (COLANGELO, 2016, 275).

41 CORTE DI GIUSTIZIA, causa C-170/13, *Huawei*, cit., par. 55.
42 CORTE DI GIUSTIZIA, causa C-170/13, *Huawei*, cit., par. 54.

L'importanza della riflessione si coglie se si pensa che, secondo alcune opinioni, la Corte, trascurando i test *ITT Promedia* e *Protégé International*[43] (secondo i quali un'azione in giudizio viola l'articolo 102 solo nel caso in cui abbia natura defatigatoria e sia concepita nell'ambito di un piano volto a falsare la concorrenza), avrebbe reso possibile una disapplicazione di tali precedenti, anche in casi diversi da quelli relativi agli standard (RATO, ENGLISH, 2016, 112). Per le ragioni appena esposte, la sentenza non può ritenersi offrire indicazioni in tal senso. La Corte elabora, piuttosto, una regola speciale nell'ambito del *genus "*rifiuto di licenza", da cui poi trae l'illegittimità dell'azione inibitoria, che del rifiuto costituisce mera attuazione. L'azione inibitoria viola l'articolo 102 non in quanto abuso di posizione dominante "in sé", ma come attuazione di un abuso di posizione dominante (in senso simile pare potersi leggere JONES, 2014, 1 ss.; si v. anche MAUME, 2016, 207 ss.)[44]. Si spiega così per quale motivo la Corte ometta ogni riferimento al test *ITT Promedia* e ritenga piuttosto opportuno confrontarsi con la giurisprudenza sul rifiuto di licenza.

12. I problemi della sentenza Hawuei. Le regole elaborate dalla Corte nella sentenza in commento impongono delle osservazioni sul tema della loro applicazione pratica.

Nella maggior parte dei casi, le controversie sui brevetti essenziali non sorgono per via di un netto rifiuto del titolare. Vengono, piuttosto, effettuate comunicazioni reciproche e avviate delle trattative, che poi falliscono. In questo caso, un vero e proprio rifiuto di concludere un contratto non c'è. Se, poi, viene presentata richiesta di inibitoria, il giudice dovrà applicare le regole elaborate dalla Corte.

Il "*safe harbour*" richiede di accertare il carattere FRAND della proposta effettuata dal titolare prima di proporre l'azione in giudizio. In mancanza di una

43 TRIBUNALE DELL'UNIONE EUROPEA, causa T-111/96, *ITT Promedia,* cit.; TRIBUNALE DELL'UNIONE EUROPEA, causa T-119/09, *Protégé International*, cit.

44 La lettura qui proposta è coerente con l'approccio seguito in un altro caso. Il caso *IMS Health* riguardava un rifiuto di licenza che era stato seguito dalla presentazione di un'azione inibitoria. Nella vicenda, si prende in considerazione il carattere abusivo del rifiuto, non quello dell'azione. CORTE DI GIUSTIZIA, causa C-418/01, cit.

tale proposta, il "*safe harbour*" non può trovare applicazione e lascia spazio alla regola generale sul rifiuto. Quest'ultima impone l'accertamento che il titolare abbia rifiutato la stipulazione a condizioni "eque, ragionevoli e non discriminatorie"; si tratta di verificare, dunque, in cosa consistono queste condizioni per poi valutare se il titolare le abbia rigettate durante le trattative. In definitiva, le regole elaborate dalla Corte richiedono, nella maggior parte dei casi, la valutazione da parte del giudice del significato di FRAND.
In questo aspetto sta la più rilevante differenza tra la soluzione elaborata dalla Corte di Giustizia e quelle che erano state offerte dalla Commissione europea e dai giudici nazionali.

Tanto la Commissione quanto i giudici tedeschi avevano evitato di dare una definizione di "FRAND" per la soluzione delle controversie sui brevetti essenziali. La Commissione aveva posto l'accento sulle dichiarazioni dell'utilizzatore e sull'esistenza di tattiche dilatorie; i giudici tedeschi sul fatto che l'utilizzatore avesse assunto un ruolo attivo nelle trattative. La decisione della Corte fissa, invece, nello stesso concetto di FRAND il nucleo dell'analisi. Del concetto, però, non offre alcuna definizione, rimettendone completamente l'accertamento al giudice[45].

Un primo problema della soluzione scelta dalla Corte si coglie se si considera che il carattere abusivo dell'inibitoria è una questione che si colloca, generalmente, in sede cautelare. Per applicare le regole della Corte, il giudice cui viene richiesta l'adozione di un provvedimento d'urgenza dovrà giudicare non solo del carattere essenziale del brevetto[46], ma anche del carattere equo e

45 Il fatto che le questioni in tema di brevetti essenziali traggano origine essenzialmente dall'incertezza che circonda la nozione di FRAND è stato colto dall'Avv. Gen. Wathelet nelle sue conclusioni. Tuttavia, l'Avvocato Generale ha anche affermato che la definizione rientra «*nella competenza esclusiva delle parti e, se del caso, dei giudici civili o dei tribunali arbitrali*». Inoltre, secondo le sue Conclusioni, il problema delle inibitorie abusive potrebbe essere ridotto o evitato se le organizzazioni di standardizzazione offrissero una definizione di FRAND. Conclusioni dell'Avv. Gen. Wathelet, causa C-170/13, 20 novembre 2014, par. 9 ss. Ritiene insufficiente la clausola FRAND applicata alle negoziazioni bilaterali per affrontare il tema dei brevetti essenziali LIBERTINI, 2017, 7 ss.
46 Elemento che va verificato, perché, nella maggior parte dei casi, le organizzazioni di standardizzazione ricevono numerose segnalazioni di brevetti essenziali da parte delle imprese partecipanti e a tutte queste richiedono di assumere un impegno FRAND; ma l'organizzazione non accerta che il brevetto sia davvero essenziale: CORTE DI GIUSTIZIA, causa C-170/13,

ragionevole delle proposte effettuate durante le trattative. Si tratta di una complessa analisi dei mercati interessati e delle caratteristiche tecniche degli standard che mal si adatta ad una cognizione sommaria dei fatti[47].

Del resto, l'elemento del FRAND si presta ad essere interpretato nei modi più vari. Sono, infatti, numerose le teorie che propongono interpretazioni del concetto e queste portano spesso ad esiti contrastanti (si v., ad esempio, COMMISSIONE, *Linee direttrici,* par. 289; LEMLEY - SHAPIRO*,* 2013, 1136 ss.*;* SWANSON - BAUMOL, 2005, 1 ss. SIDAK, 2013, 913 ss*.* FRANZOSI, 2015, 259 ss*.* GHIDINI, TRABUCCO, 2017; PADILLA - O'DONOGHUE, 2013, 689)[48]. E' pertanto ben possibile che, nell'applicare la regola della Corte, i vari giudici nazionali decidano in maniera diversa sui medesimi fatti.

Il timore è che la Corte, nel tentativo di offrire certezza, abbia piuttosto complicato le cose, elaborando una soluzione incompleta e incerta[49].

Huawei, cit., par. 19-20 e 69; L'accertamento è complesso e impone di verificare che non vi siano modi di produrre in conformità dello standard diversi dall'utilizzo del brevetto. Probabilmente la sede più adatta per questo accertamento è il procedimento principale.

47 Sul tema delle difficoltà di accertare il FRAND in sede cautelare e sulla necessità di concentrarsi sulle trattative e la buona fede delle parti si v. TRIB MILANO, 6 dicembre 2011, cit. A complicare la valutazione sta il fatto che, nella prassi, le negoziazioni non riguardano un solo brevetto ma l'intero portafogli brevettuale del titolare. In questi casi, stabilire se le proposte sono FRAND o meno diventa particolarmente complesso.

48 Le incertezze insite nel calcolo del FRAND sono state sottolineate nella recente "roadmap" della Commissione (COMMISSIONE EUROPEA, *Standard essential patents for a European digitalised economy,* 10 apr 2017, disponibile su https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-1906931_en).

La giurisprudenza americana ha affrontato il tema, ad esempio, in *Georgia Pacific Corp. V. United States Plywood Corp.,* 318 F. Supp. 1116 (S.D.N.Y. 1970); *Microsoft v. Motorola,* 2013 US Dist. LEXIS 60233 (W.D. Wash., 2013); *In re Innovatio IP Ventures,* 2013 U.S. Dist. LEXIS 144061 (N.D. Ill. 2013). Per un'analisi di questa giurisprudenza v. COLANGELO, 2014, 435 ss. Sulla centralità della clausola FRAND nelle controversie tra titolari e utilizzatori si v. anche la postfazione di GHIDINI in *Concorrenza e comportamenti escludenti nei mercati dell'innovazione,* a cura di Colangelo, Falce, 2017, 195 ss.

49 Questo limite emerge chiaramente da alcune vicende tedesche successive alla sentenza in esame. In uno di questi (LANDGERICHT DÜSSELDORF, 4a O 93/14 and 4a O 144/14, 3 novembre 2015, *Sisvel v. Haier*), un'impresa titolare di brevetti essenziali nel settore delle telecomunicazioni chiedeva un provvedimento inibitorio contro alcuni utilizzatori dello standard in questione. Questi ultimi avevano ricevuto delle comunicazioni e avevano risposto con una controproposta, a sua volta rifiutata dal titolare. I contraffattori si difendevano sostenendo che la proposta del titolare non fosse FRAND. Il giudice ha applicato il "*safe harbour*" della sentenza *Huawei*. Ma, a questo fine, ha ritenuto di non dover valutare il carattere FRAND della proposta, essendo sufficiente a negare applicazione all'articolo 102 il fatto che i contraffattori non avessero fornito in tempi brevi una garanzia appropriata. In altri termini, il giudice ha interpretato il "*safe harbour*" al contrario (Per un caso simile, si v. LANDGERICHT MANNHEIM, 2 O 106/14, 27 novembre 2015, *Saint Lawrence v. Deutsche Telekom)*. La Corte d'appello ha però sospeso

E' incompleta, in primo luogo, laddove elabora un "*safe harbour*", in qualità di valvola di sicurezza del sistema, ma lo fonda su un elemento di incertezza, anziché su elementi oggettivi. Un'alternativa era forse quella di applicare un "*safe harbour*" al titolare che avesse avanzato proposte al contraffattore, avesse risposto prontamente alle controproposte e, in caso di perdurante disaccordo sulle condizioni del contratto, avesse proposto di rivolgersi ad un terzo indipendente, vincolandosi a rispettare la soluzione offerta da questi sul tema del FRAND[50]. In queste condizioni, il comportamento del titolare non può costituire né un abuso "escludente", dato che rifiuto non c'è, né di "sfruttamento", in quanto il titolare rinuncia, addirittura, a definire le condizioni del contratto.

La decisione appare incompleta anche dove pone una regola generale in materia di standard. Che sia corretto porre a fondamento dell'abuso il rifiuto di stipulare il contratto a condizioni "eque, ragionevoli e non discriminatorie" è fuor di dubbio. Tuttavia, l'applicazione di questa regola costringe ad accertare il significato di condizioni FRAND per desumerne la scorrettezza del comportamento del titolare.

13. Inversione dell'analisi. Un passaggio ulteriore nella definizione della regola generale avrebbe potuto essere quello di suggerire un'inversione dell'analisi. Si può presumere, infatti, che se il titolare del brevetto assume un

---

l'inibitoria sulla base del fatto che la sentenza avrebbe applicato in maniera manifestamente errata il giudizio *Huawei.* (OBERLANDESGERICHT DÜSSELDORF, I-15 U 65/15 and I-15 U 66/15, 13 gennaio 2016). Un altro caso in cui il giudizio della Corte è stato applicato in modo da evitare l'analisi del concetto di FRAND è LANDGERICHT MANNHEIM, 7 O 66/15, 29 gennaio 2016, *NTT DoCoMo v. DoCoMo v. HTC Germany.* Per un caso in cui il giudice ha affrontato il tema del carattere FRAND della proposta del titolare si v. LANDGERICHT DÜSSELDORF, 4a O 73/14, 4a O126/14, 4a O 127/14, 4a O 128/14, 4a O 129/14, 4a O 130/14, 31 maggio 2016, *Saint Lawrence v. Vodaphone.* Sul tema si v. COLANGELO, 2017, 169 ss.

Un'intepretazione flessibile della sentenza *Huawei* è stata adottata nella decisione inglese HIGH COURT OF JUSTICE, *Unwired Planet,* cit., par. 741.

Sul tema dei punti lasciati aperti dalla sentenza *Huawei* v. COMMISSIONE EUROPEA, *Standard essential patents for a Euroepan digitalised economy,* 10 apr 2017, disponibile su https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-1906931_en.

50 La Corte prevede il ricorso al giudizio di un terzo indipendente solo come una possibilità per le parti che non arrivino ad un accordo. Non include, però, tale accordo nel "*safe harbour*", come dimostra il fatto che non richiama il punto nella parte finale del giudizio in cui espone la regola.

comportamento evidentemente sleale o ambiguo durante le trattative, egli intenda ottenere un risultato non FRAND. In questo caso, il titolare sta rifiutando di stipulare un contratto a condizioni "eque, ragionevoli e non discriminatorie" e, dunque, la sua successiva azione costituisce una violazione dell'articolo 102. Ne deriva che, laddove il titolare tenga un comportamento non solo tale da non soddisfare il "*safe harbour*", ma anche in evidente contrasto con quell'impegno di cooperazione che è la clausola FRAND (PETIT, 2017)[51], si può presumere che la sua azione inibitoria successiva violi l'articolo 102, senza necessità di stabilire se le *royalties* proposte fossero FRAND. A tal proposito, l'analisi, almeno in un primo momento, dovrebbe concentrarsi su elementi oggettivi, relativi al comportamento tenuto dal titolare durante le trattative. Si pensi, ad esempio, al fatto che l'azione inibitoria sia stata proposta in seguito all'abbandono ingiustificato delle trattative da parte del titolare; oppure al fatto che il titolare abbia agito per l'inibitoria senza rispondere alle controproposte del contraffattore. Si pensi, ancora, all'insistenza ingiustificata del titolare su alcuni punti della proposta, alla minaccia di agire in giudizio nei confronti della controparte, al rifiuto di prendere in considerazione controproposte o alla mancanza di trasparenza durante le trattative. Potrebbe anche essere rilevante il fatto che il titolare rifiuti la proposta concreta dell'utilizzatore di rivolgersi ad un terzo indipendente per la definizione delle *royalties* FRAND.

Dall'altro lato, anche il comportamento del contraffattore può essere rilevante nell'applicare la regola elaborata dalla Corte. Infatti se l'utilizzatore assume un comportamento sleale e dilatorio di fronte ad una proposta di licenza del titolare oppure rifiuta ingiustificatamente la proposta del titolare di rimettere ad un terzo indipendente la definizione di FRAND, si può presumere che egli stia tentando di ottenere un risultato non FRAND o, meglio, sub-FRAND. L'azione inibitoria del titolare non costituisce, in questo caso, rifiuto di concedere una licenza FRAND ma rifiuto di accettare una licenza sub-FRAND, sicché non viola l'articolo 102.

51 Per una lettura dell'impegno FRAND come un obbligo di collaborazione, più che come un impegno di prezzo si v. HIGH COURT OF JUSTICE, *Unwired Planet,* cit., par. 806.

Alla luce di queste considerazioni, l'esistenza di un rifiuto di stipulare un contratto a condizioni FRAND potrebbe essere desunta anche dal solo comportamento scorretto delle parti. Pertanto, l'analisi, anziché sul carattere FRAND delle proposte del titolare, dovrebbe concentrarsi, almeno in un primo momento, sul comportamento assunto complessivamente dalle parti durante le trattative.

Può anche accadere, comunque, che entrambe le parti tengano un comportamento che, pur non essendo tale da rientrare nel "*safe harbour",* sia apparentemente corretto e, tuttavia, non si raggiunga un accordo sul livello delle *royalties*: se la questione non viene rimessa ad un terzo, non si arriva alla stipulazione di un contratto. In questa situazione, per valutare l'esistenza di un rifiuto di concludere il contratto a condizioni FRAND, al giudice non resta che valutare le condizioni contrattuali proposte prima del fallimento delle trattative.
Si è già detto della difficoltà di realizzare questa valutazione per un giudice in sede cautelare, della divergenza di opinioni sul metodo corretto di calcolo delle *royalties* FRAND e del rischio di decisioni contrastanti nei diversi Stati membri[52].

Il giudice nazionale chiamato a effettuare questa valutazione dovrà probabilmente rivolgersi alla consulenza di un perito, il quale definisca il parametro su cui valutare il carattere "equo e non discriminatorio" delle *royalties*. Al riguardo, vale la pena di porsi il dubbio se non sia raccomandabile che il giudice nazionale si rivolga per la valutazione del significato di FRAND a determinate professionalità riconosciute dalle autorità antitrust o dalla Commissione europea [53]. Tale soluzione, che può derivare solo da una scelta

52 La difficoltà dell'analisi risiede, principalmente, nel fatto che la definizione di cosa sia FRAND richiede di valutare che, da una parte, il livello di royalties proposto sia tale da costituire un premio-incentivo adeguato per l'attività inventiva del titolare e che esso non costituisca il frutto dello sfruttamento del potere di mercato acquisito con l'inserimento del brevetto nello standard; dall'altra, il livello di royalties non deve essere tale da costituire un disincentivo per le altre imprese a ripensare lo standard e a sostituirlo, se necessario, con tecnologie superiori. In altre parole, la fissazione delle royalties FRAND richiede una complessa analisi degli incentivi dei partecipanti all'attività innovativa, in termini di concorrenza dinamica e progresso tecnologico dei mercati.
53 La soluzione di coinvolgere nella nomina del perito un'autorità antitrust è in parte ispirata alle decisioni dell'AGCM nella vicenda *Merck* (v. decisione dell'AGCM, caso *Merck/Principi attivi,*

spontanea del giudice, potrebbe avere il merito non solo di permettere una definizione accurata di FRAND, ma anche quella di realizzare un certo grado di "centralizzazione" della questione, evitando il proliferare di interpretazioni diverse di FRAND.

14. Onere della prova e posizione dominante. La sentenza offre alcuni spunti di riflessione su altri aspetti controversi della materia degli standard.

Un primo tema è quello dell'onere della prova. Sul tema, la Commissione europea aveva operato un'inversione dell'onere probatorio nei confronti del titolare del brevetto. In particolare, secondo la Commissione deve ricadere sul titolare del brevetto la prova del fatto che, nel caso concreto, il contraffattore non fosse disposto a stipulare il contratto. Alla Commissione o al contraffattore spetterebbe solo la prova che il comportamento del titolare sia avvenuto nel contesto della standardizzazione produttiva e l'esistenza di un impegno FRAND[54].

Nella decisione in commento, la Corte tace sul tema dell'onere probatorio. Il principio vigente in materia di abuso di posizione dominante pone sulla Commissione l'onere di provare gli elementi costitutivi dell'abuso. Per come ricostruiti dalla Corte, il carattere essenziale del brevetto, l'impegno FRAND e il rifiuto del titolare sono da ritenere gli elementi costitutivi dell'abuso e, quindi, devono essere provati dalla Commissione o, comunque, dalla parte che voglia far valere l'articolo 102 in giudizio.

Un secondo tema è quella della posizione dominante del titolare di un brevetto essenziale. La Corte non affronta il tema in quanto si trattava di un

provv. 16597, 21 marzo 2007). Nella vicenda, l'Autorità aveva imposto ad un'impresa farmaceutica la stipulazione di licenze su certi principi attivi. Per il caso in cui vi fossero divergenze sulle *royalties,* era previsto che le parti rimettessero la questione ad un perito nominato dall'AGCM stessa, su parere del Ministero delle attività produttive (v. par. 18 della decisione citata).

54 Secondo la Commissione, l'elemento della "*willingness*" del contraffattore sarebbe solo una possibile giustificazione per il titolare e non uno degli elementi costitutivi della fattispecie "abuso". Le argomentazioni della Commissione sul punto sono le seguenti. Il concetto di "abuso", nel diritto antitrust, si riferisce ad elementi oggettivi della fattispecie relativi al comportamento dell'impresa dominante. Inoltre, quest'ultima deve essere in grado di valutare la legittimità del suo agire sulla base di fattori ad essa conosciuti e sotto il suo controllo, in virtù del principio della certezza del diritto (COMMISSIONE, caso *Motorola,* cit. par. 434).

punto non controverso del procedimento principale.

La questione più discussa al riguardo è se la mera titolarità di un brevetto essenziale implichi necessariamente la posizione dominante del titolare sul mercato. E' stato sostenuto che la titolarità del brevetto dia luogo ad una presunzione relativa al riguardo[55]. Secondo altri autori, invece, la posizione dominante del titolare non può ricavarsi in via automatica dalla titolarità del brevetto ma deve essere oggetto di un'analisi che tenga conto di vari elementi. Per esempio, si dà rilievo all'esistenza di altri standard, alla presenza di prodotti nel mercato a valle che non adottano lo standard interessato dal brevetto oppure all'esistenza di brevetti essenziali sullo stesso standard di titolarità di altre imprese aderenti (GERADIN, RATO, 2007 145 ss. MELI, 2014, 19 ss.; TEMPLE LANG, 2016, 595 ss.)[56].

La discussione sulla posizione dominante del titolare di un brevetto essenziale si risolve in una controversia su quale sia il mercato da prendere a riferimento per individuarvi delle pressioni concorrenziali all'attività del titolare del brevetto: solo quello a monte delle tecnologie incluse nello standard oppure anche il mercato a valle dove la condotta del titolare dovrebbe produrre gli effetti rilevanti per l'intervento antitrust? La risposta corretta sembra essere la seconda. E' solo con un attento accertamento del potere di mercato del titolare su tutti i mercati coinvolti che si riesce ad individuare i casi in cui l'esercizio del brevetto essenziale può davvero generare effetti escludenti e di ostacolo allo sviluppo dinamico dei mercati. Tanto più a seguito dell'elaborazione da parte della Corte di una regola sull'abuso che elimina, rispetto alla precedente giurisprudenza, qualsiasi analisi sugli effetti del comportamento del titolare sul mercato a valle e sullo sviluppo dinamico, dandoli per scontati (commenti sul tema della posizione dominante dei titolari dei brevetti essenziali sono espressi in MELI, 2017. V. anche AREZZO, 2017).

55 V. le Conclusioni della'Avv. Gen., cit., par. 58.
56 Al riguardo si v. anche. COMMISSIONE, *Linee Direttrici,* cit., par. 261, 269 e 294 dove la Commissione afferma che la questione del potere di mercato del titolare vada valutata caso per caso. Per un accertamento della posizione dominante in materia si v. COMMISSIONE, caso *Motorola,* cit., par. 221 ss.

Riferimenti bibliografici

E. AREZZO, *Is dominance the missing piece of the* Huawei *puzzle?,* in *Orizzonti del Diritto Commerciale,* rivista telematica I, 2017.
S. BARTHELMESS, M. DOLMANS, R. ZIMBRON, *Enforcing standard essential patents: the European Court of justice's judgment in* Huawei v. ZTE, in *Intellectual Property & Technology Law Journal,* XII, 2015.
S. BRANKIN, S. CISNAL DE UGUARTE, L. KIMMEL, Huawei/ZTE: *towards a more demanding standard of abuse in essential patent cases,* in *Journal of European Competition Law & Practice,* VII, 2016.
M. CALDERINI, A. GIANNACCARI, M. GRANIERI, *Standard, proprietà intellettuale e logica antitrust nell'industria dell'informazione,* Il Mulino, Bologna, 2005.
P. CHAPPATTE, *FRAND commitments: the case for antitrust intervention,* in *European Competition Journal,* V, 2009.
P. CHAPPATTE, *FRAND commitments and EC competition law: a rejoinder,* in *European Competition Journal,* VI, 2010.
G. COLANGELO, *Aspettando* Huawei Technologies: *standard, brevetti essenziali e impegni F/RAND,* in *Mercato concorrenza regole,* III, 2014.
G. COLANGELO, *Il mercato dell'innovazione: brevetti, standards e antitrust,* Giuffrè, Milano, 2016.
G. COLANGELO, *L'*enforcement *europeo dei brevetti essenziali dopo* Huawei, in *Concorrenza e comportamenti escludenti nei mercati dell'innovazione,* a cura di Colangelo, Falce, 2017.
J.L. CONTRERAS, *Fixing FRAND: A Pseudo-Pool Approach to Standards-Based Patent Licensing,* in *Antitrust Law Journal,* I, 2013.
F. DENOZZA, *The future of antitrust: concern for the real interests at stake or etiquette for oligopolists?,* in *Orizzonti del Diritto Commerciale,* rivista telematica, I, 2017.
M. DOLMANS, *Standards for standards,* in *Fordham International Law Journal,* 2002.
J. DREXL, *Intellectual property in competition: how to promote dynamic competition as a goal,* in *More common ground for international competition law,* a cura di DREXL, GRIMES, JONES, PERITZ, SWAINE, 2011.
J. FARRELL-J. HAYES-C. SHAPIRO-T. SULLIVAN, *Standard setting, patents and hold up,* in *Antitrust Law Journal,* III, 2007.
M. FRANZOSI, *Royalty per uso di brevetto standard:* but for Georgia Pacific, apportionment, in *Riv. Dir. Ind.,* I, 2015.
D. GERADIN-M. RATO, *Can Standard-Setting lead to Exploitative Abuse? A Dissonant View on Patent Hold-Up, Royalty Stacking and the Meaning of FRAND,* in *European Competition Journal,* III, 2007.
D. GERADIN-M. RATO, *FRAND commitments and EC competition law: a reply to Philippe Chappatte,* in *European Competition Journal,* VI, 2010.
D. GERADIN, *Patent assertion entities and EU competition law,* George Mason Law & Economics Research Paper n. 16-08, 2016, disponibile su papers.ssrn.com.
G. GHIDINI-V. FALCE, *Intellectual property on communication standards: balancing innovation and competition through the essential facilities doctrine,* in *Diritto d'autore*, 2001.
G. GHIDINI, *Alcuni recenti orientamenti interpretativi in tema di* intersection *tra PI e antitrust,* in *Rivista Italiana di Antitrust,* II, 2015.
G. GHIDINI-G. TRABUCCO, *Il calcolo dei diritti di licenza in regime FRAND: tre criteri pro-concorrenziali di ragionevolezza,* in *Orizzonti del Diritto Commerciale,* rivista telematica, I, 2017.
M. GRANIERI, *Attività di standardizzazione, diritti di proprietà intellettuale e antitrust,* in *Riv. Dir. Ind.,* I, 2004.
K. GUPTA, *The patent policy debate in the high-tech world,* in *Journal of Competition Law and Economics,* IV, 2013.
M. JACOBS-F. HÜBENER, *SEP or non SEP? Open questions after Huawei/ZTE,* in *European Competition law Review,* I, 2016.
A.JONES, *Standard essential patents: FRAND commitments, injunctions and the smartphone war,* in *European Competition Journal,* X, 2014.

T. KORBER, *Abuse of dominant position by legal actions of owners of standard-essential patents:* Huawei Technologies Co. Ltd v. ZTE Corp., in *Common Market Law Review,* 2016.
P. LAROUCHE-N. ZINGALES, *Injunctive relief in disputes related to standard essential patents: time for the CJEU to set fair and reasonable presumptions,* in *European Competition Journal,* X, 2014
M. A. LEMLEY, *Intellectual property rights and standard setting organizations,* in *California Law Review,* 2002.
M. A. LEMLEY-C. SHAPIRO, *Patent hold up and royalty stacking,* in *Texas Law Review,* 2007.
M. A. LEMLEY-C.SHAPIRO, *A simple approach to setting reasonable royalties for standard essential patents,* in *Berkeley Technology Law Journal,* 2013.
J. LERNER-J. TIROLE, *Standard essential patents,* in *Journal of Political Economy,* 123, 2015.
M. LIBERTINI, *Autonomia individuale e autonomia d'impresa,* in *I contratti per l'impresa. Produzione, circolazione, gestione, garanzia,* a cura di MAUGERI, GITTI, NOTARI, Bologna, 2013.
M. LIBERTINI, *Diritto della concorrenza dell'Unione Europea,* Giuffrè, Milano, 2014.
M. LIBERTINI, *Brevi riflessioni sulla sentenza* Huawei *(Corte di Giustizia C-170/13). Verso una regolazione delle licenze FRAND di "standard essential patents",* in *Orizzonti del Diritto Commerciale,* I, 2017.
D. LICHTMAN, *Understanding the FRAND commitment,* in *Houston Law Review,* 2010.
M. LO BUE, *Are these cartels? Price guidelines adopted by standard setting organizations,* in *Journal of European Competition Law and Practice,* VII, 2016.
B. LUNDQVIST, *The interface between EU competition law and standard essential patents – from* Orange Book Standard *to the* Huawei *case,* in *European Competition Journal*, II, 2015.
M. MARINIELLO, *Standard setting abuse: the case for antitrust control,* in *Bruegel Policy Brief,* I, 2013
M. MAUGERI, *Standardizzazione e disciplina del contratto: i F/RAND committments,* in *Annuario del Contratto 2013,* diretto da D'ANGELO, ROPPO, 2014.
P. MAUME, Huawei/ZTE, *or, how the CJEU closed the* Orange Book, in *Queen Mary Journal of Intellectual Property,* VI, 2016.
V. MELI, *Standard, standardizzazione e applicazione dell'articolo 102 TFUE ai conflitti su licenze relative a diritti di proprietà intellettuale,* in *Orizzonti del Diritto Commerciale,* 2014.
V. MELI, *The CJEU judgement in the* Huawei/ZTE *case: getting around the problem of FRAND commitments and competition law,* in *Orizzonti del Diritto Commerciale,* rivista telematica, I, 2017.
J. S. MILLER, *Standard setting, patents, and access lock-in: RAND licensing and the theory of the firm,* in *Indiana Law Review,* 2007.
G. MUSCOLO, *The Huawei case. Patents and competition reconciled?,* in *Orizzonti del Diritto Commerciale,* rivista telematica, I, 2017.
C. OSTI, *Il caso Huawei: ancora sul diritto della concorrenza come clausola generale del diritto civile,* in *Orizzonti del Diritto Commerciale,* rivista telematica, I, 2017.
J. PADILLA-R. O'DONOGHUE, *The law and economics of article 102 TFEU,* Ofxord and Portland, Oregon, Hart publishing, 2013.
R. PARDOLESI-M. GRANIERI, *Di regolazione, antitrust e diritti di proprietà industriale,* in *Mercato Concorrenza Regole,* 2004.
N. PETIT, *Injunctions for FRAND-pledged SEPs: the quest for an appropriate test of abuse under article 102 TFEU,* in *European Competition Journal,* vol. 9, III, 2013.
N. PETIT, *EU competition law analysis of FRAND disputes,* 2016, in *The Cambridge handbook of technical standardization law,* a cura di CONTRERAS, 2017, disponibile su www.papers.ssrn.com
P. PICHT, *The ECJ rules on standard essential patents: thoughts and issues post*-Huawei, in *European Competition Law Review,* 2016.
M. RATO-M. ENGLISH, *An assessment of injunctions, patents, and standards following the Court of Justice's* Huawei /ZTE *ruling,* in *Journal of European Competition Law & Practice,* VII, 2016.
C. SHAPIRO, *Setting Compatibility Standards: Cooperation or Collusion?*, in *Innovation Policy for the Knowledge Society,* a cura di DREYFUSS, ZIMMERMANN; FIRST, 2001.
J. G. SIDAK, *Hold up, royalty stacking and the presumption of injunctive relief for patent infringement,* in *Minnesota Law Review,* 2008.

J. G. SIDAK, *The meaning of FRAND, part 1: royalties,* in *Journal of Competition Law & Economics,* 2013.
D. G. SWANSON-W. J. BAUMOL, *Reasonable and non-discriminatory (RAND) royalties, standard selection and control of market power,* in *Antitrust Law Journal,* 2005.
D. J. TEECE-E. SHERRY, *Standard setting and antitrust,* in *Minnesota Law Review,* 2003.
D. TELYAS, *The Interface between competition law, patents and technical standards,* Wolters Kluwer, 2014.
J. TEMPLE LANG, *Standard essential patents and court injunctions in the high tech sector under EU law after* Huawei, in *J ERA Forum,* 2016.
B. VESTERDORF, *IP rights and competition law enforcement questions,* in *Journal of European Competition Law & Practice,* II, 2013.
V. ZENO ZENCOVICH, *Processi di definizione degli standard e diritti di proprietà intellettuale,* in *Riv Dir.Ind*., I, 2007.
A.S. ZOGRAFOS, *The SEP holder guide to the antitrust galaxy: FRAND and Injunctions,* in *World Competition,* 2014.

Decisioni

Georgia Pacific Corp. V. United States Plywood Corp., 318 F. Supp. 1116 (S.D.N.Y. 1970)
CORTE DI GIUSTIZIA, cause riunite C-241/91P e C-242/91P, *RTE e ITP v. Commissione*, 6 aprile 1995
TRIBUNALE DELL'UNIONE EUROPEA, causa T-111/96, *ITT Promedia contro Commissione delle Comunità europee,* 17 luglio 1998.
CORTE DI GIUSTIZIA, causa C-418/01, *IMS Health v. NDC Health,* 29 aprile 2004
TRIB. GENOVA, 8 maggio 2004, ord., in *Il Dir. Ind.*, 2005, 500, con nota di GRANIERI.
AGCM, caso *Merck/Principi attivi,* provv. 16597, 21 marzo 2007.
BGH, *Orange Book*, KZR 39/06, 6 maggio 2009.
Apple, Inc. v. Samsung Electronics Co., Ltd., No. 5:11-cv-01846 (N.D. Cal. Apr. 15, 2011) .
TRIB. MILANO, 6 dicembre 2011 (dep. Il 5 gennaio 2012) ord., in *Giur. Italiana*, 2013, 86, con nota di VALENTE.
LANDGERICHT MANNHEIM, causa *GPRS-Zwangslizenz*, 7 O 122/11, 9 dicembre 2011.
TRIBUNALE DELL'UNIONE EUROPEA, causa T-201/04, *Microsoft Corp. v. Commissione,* 17 settembre 2007.
TRIBUNALE DELL'UNIONE EUROPEA, causa T-119/09, *Protégé International contro Commissione europea,* 13 settembre 2012.
Apple v. Motorola, 869 F. Supp. 2d 901 (N.D. Ill. 2012).
COMMISSIONE EUROPEA, caso COMP/M.6381, *Google/Motorola Mobility,* 13 febbraio 2013.
FEDERAL TRADE COMMISSION, *In the matter of Motorola Mobility LLC and Google Inc.*, dkt. C-4410, FTC file n. 121-0120, 24 luglio 2013.
Microsoft v. Motorola, 2013 US Dist. LEXIS 60233 (W.D. Wash., 2013).
In re Innovatio IP Ventures, 2013 U.S. Dist. LEXIS 144061 (N.D. Ill. 2013).
Apple v. Motorola, 757 F. 3d 1286 (Fed. Circ. 2014).
COMMISSIONE EUROPEA, caso AT.39939, *Samsung*, 29 aprile 2014.
COMMISSIONE EUROPEA, caso AT.39985, *Motorola,* 29 aprile 2014.
CORTE DI GIUSTIZIA, Causa C-170/13, *Huawei v. ZTE,* 16 luglio 2015
LANDGERICHT DÜSSELDORF, 4a O 93/14 and 4a O 144/14, 3 novembre 2015, *Sisvel v. Haier.*
LANDGERICHT MANNHEIM, 2 O 106/14, 27 novembre 2015, *Saint Lawrence v. Deutsche Telekom.*
OBERLANDESGERICHT DÜSSELDORF, I-15 U 65/15 and I-15 U 66/15, 13 gennaio 2016.
LANDGERICHT MANNHEIM, 7 O 66/15, 29 gennaio 2016, *NTT DoCoMo v. DoCoMo v. HTC Germany.*
LANDGERICHT DÜSSELDORF, 4a O 73/14, 4a O126/14, 4a O 127/14, 4a O 128/14, 4a O 129/14, 4a O 130/14, 31 marzo 2016, *Saint Lawrence v. Vodafone.*
HIGH COURT OF JUSTICE, *Unwired Planet v. Huawei,* 5 aprile 2017.

Altre Fonti

Linee Direttrici sull'Applicabilità dell'Articolo 101 del Trattato sul Funzionamento dell'Unione Europea agli Accordi di Cooperazione Orizzontale, 2011/C 11/01.
REGOLAMENTO N. 1025/2012 del Parlamento Europeo e del Consiglio.
FTC, *Statement In the matter of Google Inc.,* FTC file n. 121-0120, 3 gennaio 2013.
ETSI, *Guide on Intellectual property rights*, 2013.
COMMISSIONE EUROPEA, *Patents and Standards: a modern framework for IPR-based standardization, final report*, 2014.
MEMO/14/322, *Antitrust Decisions on Standard Essential Patents - Motorola Mobility and Samsung- Frequently Asked Questions,* 29 aprile 2014.
Conclusioni dell'Avv. Gen. Whatelet, in causa C-170/13, *Huawei,* 20 novembre 2014.
COMMISSIONE EUROPEA, *Independent Review of the European Standardization System: Final Report,* 2015.
COMMISSIONE EUROPEA, *Standard essential patents for a European digitalised economy,* 2017.

Inquadramento sistematico e primi sviluppi empirici delle società benefit

di **CORINNA TARLANTINI**

Abstract

A year and a half ago, on December 28 of 2015, the stability law (Legge di Stabilità 2016) has established in the Italian legal system the so-called Benefit Corporation.
Through this act, the legislator aimed to introduce in Italy the outcome of current changes in the theoretical business framework of reference.
In particular, the Benefit Corporation, thanks to its hybrid nature, combines profit and non-profit-making.
The aim of this document is to provide an analysis of the Benefit Corporation critical and innovative distinguishing traits of utmost importance, by emphasizing their potential side effects; and, to produce a current picture, based on updated data, of the actual level of spread and development of this new way of doing business

1. Introduzione. Con la legge di stabilità del 2016[1], sulla scia della *Benefit Corporation,* nata nel 2010 negli Stati Uniti, è stata introdotta in Italia una nuova veste giuridica per le imprese: la c.d. "Società Benefit".

1*Legge. n.208 del 28 dicembre 2015, Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge di stabilita' 2016). (15G00222) (GU Serie Generale n.302 del 30-12-2015 - Suppl. Ordinario n. 70) Art.1, comma 376 «Le disposizioni previste dai commi dal presente al comma 382 hanno lo scopo di promuovere la costituzione e favorire la diffusione di societa', di seguito denominate "societa' benefit", che nell'esercizio di una attivita' economica, oltre allo scopo di dividerne gli utili, perseguono una o piu' finalita'di beneficio comune e operano in modo responsabile, sostenibile e trasparente nei confronti di persone, comunita', territori e ambiente, beni ed attivita' culturali e sociali, enti e associazioni ed altri portatori di interesse».*

Il legislatore italiano ha introdotto, promosso e disciplinato, con una certa ambizione e fiducia, una forma ibrida[2] di impresa denominata “Società Benefit”, potenzialmente idonea a superare la dicotomia tra gli obiettivi propri di una società *for profit* e quelli di una società *non profit.* Si assiste, infatti, alla rottura dell’incompatibilità tra impresa speculativa e non speculativa mediante un intervento normativo effettuato direttamente sulla realtà delle imprese *profit*, e non viceversa (MOSCO, 2017). In altri termini, nella Società Benefit, al perseguimento dell'egoistico, seppur intrinseco, interesse dell'imprenditore alla massimizzazione del profitto e alla conseguente ripartizione degli utili tra i soci, si affianca il perseguimento di una o più finalità di beneficio collettivo e/o pubblico. Trattasi, pertanto, di un nuovo modo di fare impresa frutto della consapevolezza di dover operare in maniera “sociale” e “sostenibile” e di rafforzare la c.d. responsabilità sociale dell'impresa (“*Corporate Social Responsibility*”), in linea con le attuali esigenze emerse anche, e soprattutto, su impulso dell'Unione Europea (v. Commissione delle Comunità Europee, Libro Verde, *Promuovere un quadro europeo per la responsabilità sociale delle imprese*, (COM), 2001). Infatti, ad oggi, anche le società lucrative sono chiamate ad interessarsi a pratiche aziendali volte a soddisfare interessi generali e sociali (MOSCO, 2017).

La principale caratteristica di tale forma di impresa è la ricerca di un bilanciamento, tutt'altro che semplice, tra interessi opposti. Si può parlare di una «*hybrid legal form to meet the needs of hybrid business» (*MCDONNEL, 2014*)*, ovvero di una forma ibrida di impresa che, al fine di conseguire il summenzionato bilanciamento di interessi, legittima gli amministratori a sacrificare in parte la “*profit maximization” (“shareholeder value”)* per il perseguimento del beneficio comune, la “*dual mission”,* prefiggendosi l'obiettivo di generare un impatto positivo sull'ambiente circostante e su tutti i potenziali portatori di interesse (“*stakeholders value*”). Stiamo assistendo, quindi, ad un mutamento del paradigma economico e imprenditoriale di riferimento che

2 Per natura ibrida, come verrà più in dettaglio esposto, si intende un modello di impresa che persegue finalità sociali, pur mantenendo a pieno uno scopo lucrativo.

risponde alle nuove esigenze dei consumatori: consumatori responsabili che scelgono i prodotti offerti da imprese concorrenti, non più solo in base al prezzo e alla qualità dei prodotti stessi, ma anche, e a volte soprattutto, in base al loro *background* e alle scelte di produzione e di impatto sociale-ambientale effettuate delle singole imprese. Siamo in un'era *post* fordista (v. Sentenza del 1919 all'esito del processo Dodge vs Ford; CASTELLANI, DE ROSSI, RAMPA, 2016, «*sentenza, che ha consolidato la posizione della "shareholder supremacy", con la quale si stabilì che gli azionisti avevano il diritto a massimizzare, con ogni modo lecito, i propri profitti»*), in cui per "sviluppo" deve intendersi una produzione del valore economico direttamente proporzionale a quella di valore sociale (PAGAMICI, 2016).

In fase iniziale è sorto spontaneo interrogarsi su quale potesse essere il vantaggio nella scelta di vincolarsi volutamente a destinare una parte delle proprie risorse al perseguimento di una o più *dual mission,* senza, tuttavia, poter beneficiare di alcuna forma diretta o indiretta di agevolazione fiscale (sembrerebbe, infatti, riproporsi il medesimo problema che ha in parte determinato l'insuccesso dell'impresa sociale[3]) (RACUGNO, 2009; forma giuridica di impresa introdotta con il Decreto Legislativo 24 marzo 2006, n. 155 - *Disciplina dell'impresa sociale, a norma della legge 13 giugno 2005, n. 118*, pubblicato nella Gazzetta Ufficiale n. 97 del 27 aprile 2006). Al riguardo, è stata formulata una prima risposta: dal *self-restraint* caratterizzante tale nuova veste giuridica delle imprese deriverebbe un ritorno positivo in termini di reputazione e di immagine commerciale, non solo presso il pubblico dei consumatori, ma anche di tutti gli *stakeholders,* i quali potrebbero associare al marchio di "Società Benefit" una serie di condotte virtuose idonee a rendere tale società maggiormente competitiva sul mercato.

A distanza di circa un anno e mezzo dal suo esordio, è possibile non solo inquadrare l'istituto di recente introduzione nei suoi aspetti maggiormente caratterizzanti e problematici, ma analizzare, altresì, l'attuale stato di diffusione

3L'impresa sociale ha il divieto di distribuire gli utili, avanzi di gestione, fondi o riserve in favore di amministratori, soci, lavoratori o collaboratori.

in Italia delle Società Benefit. A tal fine sono stati raccolti ed esaminati i dati numerici maggiormente rappresentativi dell'effettivo successo in Italia di tale veste giuridica, da un punto di vista sia quantitativo sia qualitativo, ovvero dei settori economici e delle forme di impresa interessate ad operare sul mercato come Società Benefit.

2. Eelementi chiave della forma "ibrida" di impresa della società benefit. 2.1 *Dual Mission* come ulterior oggetto sociale. La Legge di Stabilità 2016, lo ricordiamo, prevede due requisiti essenziali, intrinsecamente collegati, affinché una società possa avvalersi della veste giuridica in esame: *i)* un beneficio comune da perseguire, *ii)* un modo di operare responsabile, sostenibile e trasparente.

A tal fine, il legislatore ha fornito una definizione piuttosto ampia e generica sia di "beneficio comune", descrivendolo come «*il perseguimento, nell'esercizio dell'attivita' economica delle societa' benefit, di uno o piu' effetti positivi, o la riduzione degli effetti negativi*[4] *su una o piu' categorie di cui al comma 376»* (V. Legge di stabilità 2016, art.1, comma 378), sia delle categorie dei potenziali beneficiari della condotta responsabile di una Società Benefit[5]. La natura estesa, per non dire fumosa, del concetto di "beneficio comune" non costituirebbe alcun problema se non fosse che una Società Benefit può incorrere in azioni e/o sanzioni (per pubblicità ingannevole, pratiche commerciali scorrette o concorrenza sleale) qualora non dovesse perseguire le

4 Dalla definizione emerge come l'impatto della società sui potenziali portatori di interesse non deve essere necessariamente positivo, ma può consistere anche in una mera limitazione delle esternalità negative che potrebbero scaturire dall'esercizio dell'attività principale, ovvero quella economica, della società stessa.

5 L'agire responsabile, sostenibile e trasparente mira a determinare un impatto positivo (o ridurre quelli negativi) su «*persone, comunità, territori e ambiente, beni ed attività culturali e sociali, enti e associazioni ed altri portatori di interesse* [*stakeholders*]» (v. Legge di stabilità 2016, art.1, comma 376). E' un'elencazione meramente esemplificativa talmente ampia da poter ricomprendere potenzialmente tutti i soggetti, sia persone fisiche che giuridiche, di un ordinamento, nonché tutti i beni giuridicamente tutelati. Al riguardo, per "portatori di interessi" devono intendersi «*il soggetto o i gruppi di soggetti coinvolti, direttamente o indirettamente, dall'attività della società di cui al comma 376, quali lavoratori, clienti, fornitori, finanziatori, creditori, pubblica amministrazione e società civile*» (v. Legge di stabilità, art. 1, comma 379).

finalità di beneficio comune o operare in violazione dei principi di correttezza e trasparenza richiesti.

Alla luce di quanto sopra, è sorto spontaneo chiedersi se vi debba essere un legame, o comunque una continuità, tra le finalità di beneficio comune e l'attività economica propria della Società Benefit. Sebbene non vi sia un espresso divieto in un senso o nell'altro, sarebbe sicuramente più coerente con la volontà del legislatore richiedere la sussistenza di un legame[6]. Infatti, la coerenza tra l'attività di impresa prevista nell'oggetto sociale e la finalità di beneficio comune rende l'impegno sociale assunto dalla società più credibile e disinteressato agli occhi degli *stakeholders* e dei soci.

La *dual mission* deve essere prevista dai soci nell'atto costitutivo o nello statuto, al momento della nascita della società o nel corso della vita della stessa, mediante l'indicazione nell'oggetto sociale, oltre all'attività economica produttiva di utili, delle «*finalità specifiche di beneficio comune che intende perseguire*» (v. Legge di stabilità 2016, art.1, comma 379)

L'individuazione dell'oggetto sociale e, quindi, del tipo di attività economica che una società si prefigge di perseguire, costituisce uno dei contenuti "minimi" dell'atto costitutivo (v. art. 2328, n.3 c.c. "*Atto costitutivo*"). Trattasi di un'indicazione di particolare rilievo organizzativo per la società (v. BUONOCORE, CAPO, 2016). In particolare, l'indicazione dell'oggetto sociale (attività commerciale e non) mira a soddisfare l'esigenza di garantire che l'attività della società non si discosti dalla volontà originaria manifestata dalla compagine sociale nonché l'esigenza di delimitare, nell'interesse dei soci, le condizioni di rischio dell'investimento effettuato (v. G.F. CAMPOBASSO, M. CAMPOBASSO, 2015). L'indicazione quanto più precisa dell'oggetto sociale è requisito ancor più essenziale per la veste giuridica in esame. Mediante tale previsione vengono infatti individuati i soggetti beneficiari nei confronti dei quali la società deve garantire trasparenza e fornire tutte le informazioni necessarie

6 L'esempio più lampante potrebbe essere quello di una società che si prefigge l'obiettivo di ridurre le esternalità negative sull'ambiente in cui opera, o di salvaguardare la salute della comunità circostante, adottando materiali e metodi di produzione ecocompatibili, sostenendo, pertanto, maggiori costi a discapito dell'utile complessivo dell'impresa.

ad esercitare un controllo sull'operato della società stessa. Inoltre, qualora la finalità statutaria non dovesse essere effettivamente perseguita, il legislatore ha previsto l'applicazione di specifiche sanzioni (v. Legge di stabilità 2016, art.1, comma 384). Per le summenzionate ragioni, l'attività e le finalità che la società si prefigge di perseguire devono essere indicate il più dettagliatamente possibile al fine di: evitare abusi, consentire una concreta azione sanzionatoria e circoscrivere, eventualmente, la responsabilità degli amministratori. Infatti, ad ogni finalità di beneficio comune, come individuata dai soci nell'atto costitutivo, corrisponde l'obbligo in capo agli amministratori di realizzarla, svolgendo, a tal fine, la propria attività gestionale in modo responsabile, sostenibile e trasparente.

Alla luce di quanto sopra, a differenza di quanto previsto dalle leggi di alcuni Stati nord-americani che consentono alle B*enefit Corporation* di perseguire un beneficio comune di portata anche solo generale, il legislatore italiano tende a precludere alle Società Benefit la possibilità di avvalersi nell'oggetto sociale di formule eccessivamente generiche, indefinite o di mere petizioni di principio. Allo stesso modo, e per la medesima *ratio*, tali finalità non potranno essere così numerose e diverse tra loro da renderne impossibile l'effettivo perseguimento (RIOLFO, 2016).

2.2. Possibili abusi. Come più volte ribadito, tali società perseguono unitamente allo scopo della massimizzazione dei profitti mediante l'esercizio di un'attività economica, una o più finalità di beneficio comune. A differenza delle altre società, che possono certamente perseguire le summenzionate finalità senza tuttavia ricadere nel modello di impresa in oggetto, le Società Benefit, una volta individuata la *dual mission* nell'oggetto sociale, assumono un vero e proprio obbligo di coerenza e di realizzazione della stessa, sia nei confronti dei propri soci sia nei confronti di tutti i potenziali portatori di interesse.

Lo scopo “altruistico”, che caratterizza la Società Benefit e che gli conferisce maggiore competitività sul mercato, può essere esternalizzato, o comunque, può influenzare le scelte economiche e di investimento degli

stakeholders. Pertanto, il legislatore ha ritenuto necessario prevedere una disciplina volta a garantire che all'informazione "*social*", ovvero alla comunicazione a terzi di esercitare l'attività di impresa in modo vantaggioso anche per la collettività, segua una attività di gestione dell'impresa coerente con l'immagine che tale società si è in un certo senso autoconferita. Infatti, in assenza di specifici obblighi di trasparenza e pubblicità, per i consumatori e gli investitori non professionali potrebbe essere molto difficile, se non impossibile, monitorare il corretto e coerente svolgimento dell'attività della società e dei suoi amministratori.

Come vedremo, le Società Benefit, per le loro caratteristiche intrinseche, si prestano ad usi abusivi ed elusivi della normativa di riferimento a danno degli *shareholders* e *stakeholders.*

Già il semplice uso distorto o illegittimo della dicitura "*società benefit/SB*" riportata nella denominazione sociale potrebbe configurare una pratica commerciale sleale, un atto di concorrenza sleale (*ex* art. 2598 c.c.) o di pubblicità ingannevole. I consumatori, infatti, potrebbero essere invogliati ad acquistare i prodotti e/o servizi offerti da tali società, non tanto per la natura e la qualità intrinseca degli stessi, quanto per la condivisione della finalità sociale dichiaratamente perseguita. Allo stesso modo, i finanziatori, e più in generale, gli investitori potrebbero decidere di differenziare il proprio portfolio acquistando azioni o quote di partecipazione di una Società Benefit, per il solo fondamento etico-sociale su cui quest'ultima si basa.

Qualora le finalità di beneficio comune statutariamente previste non dovessero essere effettivamente realizzate, o quantomeno perseguite, la società si renderebbe in primo luogo responsabile di atti di "pubblicità ingannevole"[7]. Con comunicazioni caratterizzate da diversi profili di ingannevolezza, la Società Benefit potrebbe, infatti, influenzare gli atteggiamenti e le scelte degli *stakeholders* in relazione alla scelta dei beni o

7 Cosi il D.lgs. 74/1992, Art. 2 «*qualsiasi pubblicità che in qualunque modo, compresa la sua presentazione, induca in errore o possa indurre in errore le persone fisiche o giuridiche alle quali è rivolta o che essa raggiunge e che, a causa del suo carattere ingannevole, possa pregiudicare il loro comportamento economico ovvero che, per questo motivo, leda o possa ledere un concorrente».*

dei servizi, inducendoli in inganno circa l'effettivo perseguimento da parte della stessa di una determinata *dual mission*.

Nondimeno, si vengono a configurare anche gli estremi propri di una condotta di concorrenza sleale a danno sia dei consumatori che degli operatori economici concorrenti, i quali verrebbero resi ingiustificatamente meno competitivi sul mercato agli occhi dei consumatori.

Per l'ipotesi più estrema di abuso di tale modello di impresa, ovvero l'ipotesi del non effettivo perseguimento della *dual mission* statutariamente indicata, il legislatore ha già previsto ulteriori obblighi di trasparenza e controllo. Lo stesso, tuttavia, non può dirsi per le forme più occulte di abuso, per le quali sussistono delle evidenti lacune normative.

In particolare, la possibilità di modificare le "specifiche" finalità di beneficio comune indicate nello statuto, alla stregua della normativa vigente in materia di modifiche statutarie[8], può presentare dei risvolti negativi ed ingannevoli. L'applicabilità della normativa vigente fa sì che mediante una semplice modifica statutaria, realizzata secondo le modalità proprie del tipo societario adottato, i soci possano introdurre nuove specifiche finalità, o sopprimere in parte quelle precedentemente indicate. Per le Società Benefit, il legislatore non ha, tuttavia, né impedito né imposto la previsione di maggioranze qualificate. L'effetto potenzialmente collaterale della libertà di modificare l'oggetto sociale senza particolari limitazioni si ravvisa in tutti quei casi in cui la Società Benefit non dovesse riuscire a perseguire le finalità di beneficio comune. In tali ipotesi, pur di mantenere lo *status* di società "*benefit*" e di continuare a trarne i relativi benefici, nonché di evitare sanzioni per pubblicità ingannevole o pratiche commerciali scorrette, i soci potrebbero essere tentati di modificare o sostituire periodicamente la *dual mission,* adeguandola e aggiornandola, continuando, tuttavia, a non perseguirla (per impedimenti di natura oggettiva o per negligenza nella gestione) (RIOLFO, 2016). Così operando, la Società Benefit potrebbe, da

8 Ai sensi dell'Art. 2365 c.c. *«L'assemblea straordinaria delibera sulle modificazioni dello statuto, sulla nomina, sulla sostituzione e sui poteri dei liquidatori e su ogni altra materia espressamente attribuita dalla legge alla sua competenza».* Le modificazioni statutarie, almeno per le s.r.l., rientrano, pertanto, nella competenza dell'assemblea dei soci in sede straordinaria, con delibera approvata a maggioranza rafforzata.

un lato, celare agli occhi delle varie categorie di soggetti portatori di interessi l'uso abusivo della propria denominazione, dall'altro, ignorare i soci di minoranza che hanno espresso voto contrario ad una modifica statutaria elusiva della normativa vigente.

2.3. Marchio collettivo. Le sopradescritte ripercussioni negative scaturenti da un abuso del modello di impresa in esame, sembrerebbero in parte ricordare gli effetti collaterali di un uso distorto ed improprio del "marchio collettivo". Quest'ultimo – diversamente dal "marchio individuale" che ha quale principale funzione quella distintiva, ovvero quella di contraddistinguere i prodotti e/o servizi di una determinata impresa da quelli delle altre imprese[9] – svolge principalmente una funzione di garanzia: è un segno distintivo che mira a garantire la sussistenza di particolari caratteristiche qualitative dei prodotti e servizi di più imprese e serve a contraddistinguerli non da quelli di altre imprese, ma per la loro specifica provenienza, natura o qualità[10]. Il marchio collettivo nasce istituzionalmente per essere messo a disposizione dal titolare ad una pluralità di soggetti tra loro indipendenti e la cui precipua finalità è quella di garantire direttamente determinate caratteristiche qualitative dei prodotti contrassegnati (GALLI, 2007). In altre parole, si potrebbe conferire al marchio collettivo la veste di strumento di certificazione, più che di identificazione, di una determinata impresa. Infatti, il marchio collettivo svolge principalmente una funzione di garanzia qualitativa, in quanto garantisce che i prodotti e/o i servizi contrassegnati presentano una determinata origine, natura o qualità (VANZETTI, DI CATALDO, 2006).

9 Definizione di marchio individuale di impresa: Codice della Proprietà Industriale, Art. 7 «*Possono costituire oggetto di registrazione come marchio d'impresa tutti i segni suscettibili di essere rappresentati graficamente, in particolare le parole, compresi i nomi di persone, i disegni, le lettere, le cifre, i suoni, la forma del prodotto o della confezione di esso, le combinazioni o le tonalità cromatiche, purché siano atti a distinguere i prodotti o i servizi di un'impresa da quelli di altre imprese».*

10 Codice della Proprietà Industriale, Art. 11 «*Marchio collettivo:1. I soggetti che svolgono la funzione di garantire l'origine, la natura o la qualità di determinati prodotti o servizi, possono ottenere la registrazione per appositi marchi come marchi collettivi ed hanno la facoltà di concedere l'uso dei marchi stessi a produttori o commercianti».*

Gli imprenditori che hanno interesse ad aderire ad un marchio collettivo, al fine di fregiarsene legittimamente nell'esercizio della loro attività di impresa, devono preliminarmente dimostrare al titolare del segno distintivo di essere in possesso dei requisiti richiesti nel relativo regolamento d'uso. Avendo il marchio collettivo una funzione di garanzia e determinando nei consumatori la capacità di associare a quel segno distintivo specifici messaggi di qualità, natura o provenienza, qualora questi non dovessero essere effettivamente rispettati dell'operatore economico che si avvale del marchio collettivo, ne deriverebbe un inganno per i consumatori ed i concorrenti che dovrà essere sanzionato a tutti gli effetti.

Sotto il profilo del controllo vige una disciplina alquanto rigida. Ciò in quanto il messaggio sotteso ad un marchio collettivo è volto ad informare il pubblico dei consumatori in merito al duplice impegno dei soggetti autorizzati ad avvalersi di quel determinato segno distintivo di *a)* assicurare determinate qualità dei prodotti o servizi contrassegnati (individuate nell'apposito regolamento d'uso), *b)* di assoggettarsi ai controlli previsti nel medesimo regolamento. L'esistenza di tali controlli rappresenta un elemento essenziale del messaggio trasmesso per mezzo del marchio collettivo, in quanto «*alla funzione di garanzia cui i marchi collettivi presiedono è necessariamente inerente appunto la possibilità di controlli da parte del titolare*» (GALLI, 2010 - 2011) tanto che la mancata effettuazione degli stessi comporta la decadenza dello stesso marchio collettivo[11]. Ciò al fine di evitare l'inganno del pubblico e l'uso decettivo del marchio.

Si potrebbe, quindi, azzardare un parallelismo tra il marchio collettivo e la veste di "società benefit": la dicitura "*società benefit/SB*" riportata nella denominazione sociale potrebbe assolvere le funzioni di un segno distintivo mediante il quale gli operatori economici trasmettono il messaggio di garanzia circa le modalità e le finalità di beneficio comune perseguite nell'esercizio di un'attività di impresa di natura economica. Si presenterebbe, quindi, come una

11 Art. 14 c.p.i. 2° comma *"diritto alla registrazione". «Il marchio d'impresa decade a) se sia divenuto idoneo a trarre in inganno il pubblico, in particolare circa la natura, qualità o provenienza dei prodotti o servizi»*.

sorta di marchio collettivo al quale potrebbero aderire tutte le imprese che, nell'esercitare un'attività avente natura prettamente economica, perseguono al contempo uno specifico scopo di beneficio comune. Dalla divulgazione di un tale messaggio deriverebbe, infatti, un ritorno in termini di reputazione e di immagine per le imprese che perseguono benefici generali. È convinzione diffusa (nonché *ratio* della maggior sensibilità delle imprese alla tematica della "*Corporate Social Responsibility*"), che le relazioni socialmente ed eticamente virtuose costituiscano, per le imprese che le instaurano, degli "*intangible assets*" idonei a garantire un ritorno economico nel medio-lungo periodo mediante lo sfruttamento dei vantaggi competitivi derivanti dal rafforzamento dell'immagine e del valore dei marchi (CONTE, 2006).

Al fine di evitare che se ne faccia un uso prettamente decettivo, si potrebbe introdurre un sistema di controllo improntato a quello previsto per il marchio collettivo. In particolare, si potrebbe ricorrere alla previsione di un ente consortile avente la finalità di monitorare e garantire il rispetto da parte delle singole Società Benefit degli impegni statutariamente assunti ed esternalizzati per mezzo dell'adozione dello *status* nella denominazione sociale.

3. Possibili correttivi ad usi abusivi della società benefit. 3.1 Gli ulterior obblighi degli amministratori. *Bilanciamneto di interessi.* Per garantire l'effettivo perseguimento della *dual mission* attraverso l'esercizio dell'attività di impresa in modo «*responsabile, sostenibile e trasparente*», il legislatore ha sin da subito ritenuto necessario prevedere in capo agli amministratori nuovi ed ulteriori doveri.

In particolare, per evitare condotte opportunistiche degli amministratori a danno dei soci e, di riflesso, della società nei confronti degli *stakeholders*, il comma 380 della Legge di Stabilità 2016 prevede in capo all'organo di gestione l'obbligo di amministrare tali società «*in modo da bilanciare l'interesse dei soci, il perseguimento delle finalita' di beneficio comune e gli interessi delle categorie indicate nel comma 376, conformemente a quanto previsto dallo statuto».* Viene, così, affidato agli amministratori il difficoltoso compito di bilanciare

l'interesse dei soci alla massimizzazione del profitto con il perseguimento del beneficio comune individuato nell'oggetto sociale[12].

Tali obblighi, come vedremo troppo generici, ad un primo impatto non sembrerebbero favorire la diffusione della nuova veste di impresa. Infatti, si è sin da subito ipotizzato l'insorgere di un atteggiamento restio nell'adottare la forma di Società Benefit, ciò in quanto, il comma 381 dispone che "*L'inosservanza degli obblighi di cui al comma 380 può costituire inadempimento dei doveri imposti agli amministratori dalla legge e dallo statuto*". Pertanto, sembrerebbe che gli amministratori per un mancato o, semplicemente, errato bilanciamento degli interessi (spesso confliggenti, eterogenei e difficili da individuare) potrebbero incorrere in azioni di responsabilità; infatti, "*in caso di inadempimento degli obblighi di cui al comma 380, si applica quanto disposto dal codice civile in relazione a ciascun tipo di società in tema di responsabilità degli amministratori"*.

Sembrerebbe trattarsi di un bilanciamento di interessi assai difficoltoso all'esito del quale gli amministratori devono saper decidere quale interesse far prevalere e quale sacrificare. Tutto ciò senza che il legislatore abbia previsto un criterio guida certo a cui poter fare riferimento; criterio guida indispensabile, da un lato, per consentire agli amministratori di orientare le proprie scelte di gestione all'esito di un complesso bilanciamento di interessi, spesso tra loro inconciliabili, e dall'altro, per permettere un equo e prevedibile giudizio sull'operato degli amministratori. In ogni caso, è bene specificare che tale bilanciamento è tra interessi eterogenei dei soci stessi: ovvero l'interesse dei soci alla massimizzazione del profitto e l'altro interesse, sempre dei soci e da questi, pertanto, espressamente individuato nello statuto, alla realizzazione di uno specifico beneficio comune. In altre parole, gli amministratori sono chiamati a perseguire una duplice finalità, lucrativa e di beneficio comune, entrambe scopi primari della società: sebbene la massimizzazione del profitto continui a

12 Inoltre, per una miglior organizzazione degli assetti interni e per una ripartizione più efficiente dei compiti e delle responsabilità, il legislatore richiede l'individuazione di un «*soggetto o soggetti responsabili a cui affidare funzioni e compiti volti al perseguimento delle suddette finalità»* (v. Legge di stabilità 2016, art.1, comma 380).

ricoprire un ruolo di connaturata centralità, viene a mancare un rapporto di strumentalità tra gli stessi (COCCIOLILLO, 2017); tale rapporto è, invece, strutturalmente imposto ad alcuni enti collettivi, quali le associazioni e le fondazioni, nei quali l'attività di impresa, e quindi la massimizzazione del profitto, deve essere strumentale al perseguimento delle finalità istituzionali di impronta altruistica (MOSCO, 2017).

Per evitare che gli amministratori si trovino ad incorrere in una sorta di responsabilità oggettiva, ma al tempo stesso per garantire l'effettivo perseguimento degli obiettivi di beneficio comune, si riterrebbe opportuno introdurre degli *standard,* specifici e dettagliati, di comportamento degli amministratori, così che il mancato rispetto degli stessi sia facilmente accertabile e sia conseguenzialmente possibile dichiarare con certezza quando i soci, la società o i singoli *stakeholders* siano legittimati ad agire nei confronti degli amministratori. Negli Stati Uniti si è, infatti, sin da subito avvertita l'esigenza di liberare i *managers* da tale rischio, che nel caso di specie si traduce nell'esigenza di predeterminare i confini entro i quali poter affermare che il bilanciamento di interessi contrapposti effettuato dagli amministratori a vantaggio di alcuni portatori di interesse e a svantaggio di altri porti ad un risultato legittimo e quando, invece, tale risultato sia illecito o il frutto di *mala gestio*.

A tal riguardo è nota la già citata sentenza "*Dodge Vs Ford*" per aver espressamente sancito la *"shareholder supremacy"*[13], a seguito della quale si è assistito a numerosi casi di azioni di responsabilità esercitate nei confronti degli amministratori per aver questi ultimi violato, nell'esercizio delle proprie funzioni gestorie, il principio di massimizzazione del profitto dei soci per perseguire politiche di "*Corporate Social Responsibility"*. Al tempo vigeva uno stato di assoluta incertezza nel quale gli amministratori non avevano gli strumenti per predeterminare e prevedere quando le loro decisioni e valutazioni di

13 *«A business corporation is organized and carried on primarily for the profit of the stockholders. The powers of the directors are to be employed for that end. The discretion of directors is to be exercised in the choice of means to attain that end, and does not extend to a change in the end itself, to the reduction of profits, or to the non-distribution of profits among stockholders in order to devote them to other purposes»*

bilanciamento di interessi avrebbero costituito una violazione dei propri doveri fiduciari (un tentativo di circoscrivere la responsabilità degli amministratori è stato effettuato mediante l'introduzione dei c.d. "*constituency statutes*", atti normativi che legittimano, ma non obbligano, gli amministratori a considerare nell'esercizio delle loro funzioni sia gli interessi dei soci che quelli di altri soggetti e, pertanto, a perseguire interessi di diverse categorie di *stakeholders.* Sul punto HILLER, 2013). Proprio in tale contesto sono nate le *Benefit Corporation*, nuova forma di impresa, giuridicamente riconosciuta, volta ad agevolare la creazione di benefici non solo per gli *shareholders,* ma anche per gli *stakeholders*, attenuando in tal modo il principio della *"shareholder supremacy"* e legittimando espressamente gli amministratori a perseguire la "multipla *bottom line*" (ovvero, «*il valore economico prodotto dalla differenza tra ricavi e costi subisce l'influenza della dimensione sociale e ambientale*», CUMMINGS, 2012) a discapito della *profit maximization* (ciò nella consapevolezza che gli aspetti sociali e ambientali fossero fattori sempre più rilevanti per l'acquisizione di un maggior vantaggio competitivo di un'impresa sul mercato. Sul punto CASTELLANI, DE ROSSI, RAMPA, 2016).

Per incrementare la diffusione delle Società Benefit anche nel nostro paese, si è sin da subito pensato ad adottare quale modello le legislazioni di alcuni paesi statunitensi disciplinanti non tanto l'istituto in astratto, quanto gli aspetti attinenti il concreto funzionamento della nuova veste di impresa[14]. Inoltre, si è prospettata l'ipotesi di prevedere a livello statutario obblighi ed istruzioni più specifiche in capo agli amministratori in sede di bilanciamento di interessi;

14 Si può riportare quale esempio, la legislazione del Minnesota, che prevede specifici *standard* di comportamento per gli amministratori di una *Benefit Corporation;* in particolare, questi ultimi, al fine di adempiere ai propri doveri, in quanto amministratori di una "BC", possono legittimamente decidere di non dare priorità agli interessi economici dei soci: «*may not give regular, presumptive, or permanent priority to i) the pecuniary interests of the shareholders».* Minnesota Statute, Chapter 304A «*In discharging the duties of the position of director of a general benefit corporation, a director 1) shall consider the effects of any proposed, comtemplated, or actual conduct on: i) the general benefit corporation's ability to pursue its specific public interest; 2) may not give regular, presumptive or permanent priority to: i) the pecuniary interests of the shareholders...».*

tuttavia, trattandosi di bilanciamento intrinsecamente discrezionale, nella pratica, ciò risulta assai arduo se non impossibile[15].

Le problematiche appena esposte sembrerebbero svanire. Infatti, il legislatore italiano ha previsto alcuni strumenti di tutela per gli amministratori delle Società Benefit; strumenti idonei, di fatto, a circoscrivere quanto più possibile il rischio degli stessi di incorrere in azioni di responsabilità. In primo luogo, il bilanciamento tra scopi diversi, ma tra loro non incompatibili, legittima gli amministratori a far prevalere uno scopo sull'altro, nel caso in cui non siano entrambi perseguibili, senza che ciò si traduca in una violazione dei doveri fiduciari da parte dell'organo gestorio (MOSCO, 2017). Corollario di tale bilanciamento è la concreta possibilità che lo scopo di lucro, pur mantenendo una posizione di preminenza, possa essere di volta in volta parzialmente sacrificato. In secondo luogo, la discrezionalità gestoria del bilanciamento di interessi riconosciuta agli amministratori implica l'impossibilità di contestare le scelte gestionali per il semplice ridursi o venir meno dei risultati di natura prettamente economica (COCCIOLILLO, 2017). Infatti, stante l'impossibilità di eliminare un margine di discrezionalità nelle scelte operative dei *managers*, è opportuno avvalersi della diligenza professionale quale parametro di valutazione idoneo a circoscrivere la portata della loro responsabilità. In altre parole, gli amministratori, così come previsto dal comma 376, dovranno fondare le proprie scelte sul principio dell'agire imprenditoriale «*responsabile, sostenibile e trasparente*». Il principale orientamento giurisprudenziale esclude, pertanto, una responsabilità per *mala gestio* dell'amministratore ogniqualvolta le sue scelte di strategia aziendale si siano rivelate errate alla stregua di un giudizio *ex post;* la valutazione in merito all'effettivo rispetto dei doveri di diligenza e dell'agire informati dovrà essere effettuata alla stregua di un

15 Ciò per un duplice ordine di ragioni: i) in primo luogo, l'attività gestoria è di competenza esclusiva degli amministratori (del consiglio di amministrazione o, quando consentito dallo statuto o dall'assemblea dei soci, di un comitato esecutivo composto da alcuni componenti del consiglio di amministrazione) (v. Art. 2381 c.c. «Presidente, comitato esecutivo e amministratori delegati»), infatti i soci potrebbero non avere le conoscenze e le competenze necessarie per individuare statutariamente il corretto modus operandi dell'organo di gestione; ii) in secondo luogo, risulta difficile definire all'interno dello statuto, in aggiunta ai principi generali, delle linee guida per gli amministratori che siano sufficientemente dettagliate.

controllo *ex ante* sull'operato degli amministratori[16]. In linea con tale orientamento, non è responsabile l'amministratore che abbia diligentemente ed in modo informato bilanciato i diversi interessi in gioco privilegiando la soluzione ritenuta migliore, quest'ultima adottata in assenza di interessi personali in conflitto con quelli della società o degli *stakeholders*[17]. Infine, per quanto concerne i soggetti legittimati ad agire nei confronti degli amministratori per violazione dei doveri fiduciari, il legislatore, rinviando alle *«norme previste dal codice civile per le società di persone, capitali e cooperative»* ha escluso tale legittimazione attiva in capo ai terzi beneficiari (COCCIOLILLO, 2017).

Alla luce di quanto sopra, sebbene il legislatore, al fine di monitorare l'operato delle Società Benefit ed evitare che queste sfruttino indebitamente il relativo "marchio", abbia ampliato gli obblighi degli amministratori, nonché l'oggetto dell'azione di responsabilità nei loro confronti, il risultato potrebbe in definitiva rivelarsi opposto. Infatti, sia l'accrescimento del potere discrezionale degli amministratori, sia l'assenza di una legittimazione attiva in capo ai terzi beneficiari della *dual mission* rischiano di ridurre, di fatto, la possibilità di garantire un controllo effettivo sul loro operato.

Relazione annuale. Al fine di ridurre ulteriormente i rischi di un uso abusivo o distorto della Società Benefit, il legislatore ha previsto, apparentemente in capo alla società ma effettivamente in capo agli amministratori, l'obbligo di predisporre una relazione annuale «*concernente il perseguimento del beneficio comune, da allegare al bilancio societario».* Tale relazione ha la funzione di rendere trasparente, e quindi assoggettabile ad un

16 Sul punto, Trib. Firenze del 29 maggio 2015, Sez. Spec. Impresa, *Ilsocietario.it* 2015, 24 agosto, ha statuito che *«E' da escludersi che la verifica giudiziale dei comportamenti dell'organo amministrativo possa inoltrarsi nel campo delle scelte discrezionali, per loro natura caratterizzate da una non trascurabile componente aleatoria. Pertanto, il discrimine tra la condotto diligente e la mala gestio dell'amministratore non può sostanziarsi nella verifica ex post dei rischi connessi ad una scelta imprenditoriale risultata perdente; occorre, invece, accertare se l'amministratore, prima di prendere una certa decisione gestionale, abbia approfonditamente e adeguatamente ponderato tutti i possibili e prevedibili profili di rischio ad essa connessi, ed abbia a tal fine apprezzato altresì tutti i dati e gli elementi di valutazione concretamente acquisibili nel caso specifico».*

17 Nel caso in esame, per soluzione migliore si deve intendere la soluzione in grado compensare il sacrificio richiesto all'interesse di una categoria con un vantaggio per gli interessi di altra categoria di soggetti che può anche non coincidere con quella degli *shareholders*.

controllo interno ed esterno, il modo di operare delle imprese in termini di sostenibilità e di impatto socio-ambientale. In tal modo, il comma 382 della Legge di Stabilità introduce un nuovo obbligo in capo agli amministratori la cui violazione, a differenza degli obblighi fiduciari di cui sopra, è facilmente individuabile[18]. Perché la relazione in esame possa assolvere alla sue funzioni di garanzia e trasparenza, sono stati introdotti degli accorgimenti in termini di forma e di contenuto.

Ricordiamo, innanzitutto, che il legislatore, al fine di consentire un controllo sull'attività effettivamente svolta per il perseguimento della *dual mission* non solo da parte dei soci, ma soprattutto degli *stakeholders,* ha previsto l'obbligo di pubblicazione della relazione annuale sul sito *internet* della società, qualora esistente (v. Legge di stabilità 2016, art.1, comma 383). Ad oggi, tuttavia, non tutte le società sono munite di un proprio sito *internet*[19]. Per conferire maggior completezza ed efficacia all'obbligo in questione, nonché per maggior garanzia dei terzi, sarebbe stato forse opportuno prevedere forme alternative di pubblicità della relazione annuale, quale, ad esempio, la pubblicazione su quotidiani. In alternativa, per conferire effettività a tale obbligo, il legislatore avrebbe potuto imporre la realizzazione del sito *internet* come condizione per adottare la forma di Società Benefit. Affinché i soci in sede di approvazione del bilancio annuale e gli altri portatori di interessi con la consultazione delle relazioni debitamente pubblicate possano effettivamente svolgere un'attività di controllo sull'operato degli amministratori, per un’eventuale azione a tutela dei propri diritti ed interessi, l'organo gestorio è chiamato a redigere la relazione nel modo più tecnico e completo possibile.

18 Il mancato o non corretto adempimento di tale obbligo, comporterà una responsabilità degli amministratori, i quali potranno essere revocati e/o tenuti a risarcire i danni cagionati alla società. Tuttavia, proprio alla luce del dato letterale del comma 382 («*la società benefit redige annualmente...»*), anche la società sarà ritenuta responsabile della mancata o inesatta redazione della relazione annuale.

19 Salvo le società quotate o aperte, per le quali il legislatore ha già imposto l'utilizzo di siti internet o, in alternativa, di quotidiani per finalità di trasparenza, le altre forme di impresa non si avvalgono necessariamente di tale forma di pubblicizzazione.

Trattasi di un'ulteriore precauzione volta ad evitare che tale controllo esterno si riduca ad una mera formalità[20].

La parte della relazione maggiormente volta a consentire una vigilanza esterna sull'impatto socialmente utile conseguito da una Società Benefit, sia da parte dei soci che degli *stakeholders*, è rappresentata dalla voce *sub b)*, ovvero dalla *"valutazione dell'impatto generato"* dall'attività societaria nel perseguimento delle finalità di beneficio comune (il c.d. "*Benefit Impact Report*"). Queste informazioni, se veritiere, dovrebbero costituire l'oggetto ed il parametro del controllo effettuato sulla conformità dell'operato di una Società Benefit rispetto alle disposizioni statutarie e ai requisiti di legge. Tale impatto dovrà essere descritto e valutato dall'organo amministrativo alla stregua di uno "*Standard di Valutazione Esterno*" predisposto da un ente munito delle necessarie competenze[21]. L'intenzione del legislatore di fornire gli elementi sui quali, ed a mezzo dei quali, esercitare un controllo e, al tempo stesso, consentire una limitazione della responsabilità degli amministratori, sembra presentare alcuni limiti ed effetti collaterali.

Infatti, il legislatore si è limitato a prevedere in capo agli amministratori l'obbligo di usare, nella predisposizione della relazione annuale, *standard* e criteri valutativi predisposti da un qualsiasi (non uno in particolare) ente terzo; quest'ultimo è, quindi, chiamato esclusivamente a formulare degli *standard* di valutazione di cui le singole Società Benefit si avvarranno per descrivere la propria attività sotto il profilo dell' "impatto generato" in termini di benefici socio-ambientali. In tal modo, il legislatore ha regolarizzato solo a grandi linee un

20 In particolare, una prima parte dovrà prevedere *«la descrizione degli obiettivi specifici, delle modalita' e delle azioni attuati dagli amministratori per il perseguimento delle finalita' di beneficio comune».* Inoltre, dovranno essere indicate anche le "*eventuali circostanze"* che hanno ostacolato o rallentato il perseguimento delle specifiche *dual mission*. Quest'ultima previsione sembrerebbe porsi come una sorta di onere di motivazione in capo agli amministratori che consentirebbe agli stessi di esporre le valutazioni e l'*iter* logico adottato in sede di bilanciamento dei vari interessi contrapposti.

21 Affinché l'esito di tale resoconto sia attendibile, è necessario che l'ente preposto sia terzo, indipendente e competente e che gli standard da questo formulati siano esaustivi, adatti e/o adattabili alle singole fattispecie (v. Legge di stabilità 2016, Allegato 4 "Standard di Valutazione Esterno"). Al fine, poi, di avere una visione completa delle ripercussioni positive, la valutazione dovrà estendersi a tutte le aree potenzialmente interessate (v. Legge di stabilità 2016, Allegato 5 "Aree di Valutazione").

meccanismo di autocertificazione, effettuata dal medesimo soggetto il cui operato viene sottoposto a verifica. Oltre ai problemi sull'effettiva terzietà ed oggettività dell'autocertificazione, si potrebbero riscontrare dei problemi di natura prettamente tecnica, non essendo circostanza scontata la detenzione da parte dell'organo gestorio delle competenze e delle conoscenze adeguate per applicare correttamente i summenzionati *standard* di valutazione. Ulteriore elemento che potrebbe indebolire le funzioni di controllo, di garanzia e di limitazione della responsabilità degli amministratori affidate alla relazione in esame, è ravvisabile nell'omessa individuazione di un unico *"third-party standard-setter",* ovvero di un unico ente terzo preposto alla predisposizione degli *standard* di valutazione[22]. Potendovi essere più soggetti abilitati a predisporre *standard* di valutazione e potendo tali *standard* divergere tra di loro, la scelta di uno in luogo di altri potrebbe condurre ad esiti diversi in termini di "impatto generato". Ad esempio, si potrebbero venire a creare *standard* gerarchicamente superiori ad altri e ciò annullerebbe implicitamente la validità e l'attendibilità di quelli gerarchicamente inferiori. Inoltre, l'organo amministrativo verrebbe gravato da un ulteriore dovere: scegliere un determinato *standard* e spiegare e motivare le ragioni della propria scelta. Le difficoltà e gli inconvenienti di cui sopra evidenziano ancora di più l'esigenza di prevedere un controllo sull'attività di una SB che sia esterno, eseguito da un unico soggetto terzo e alla stregua di parametri univoci: in altre parole occorrerebbe un sistema di certificazione esterna con funzioni assimilabili al titolare di un marchio collettivo, obbligato ad effettuare controlli *ex ante* ed *ex post* sulla sussistenza dei requisiti di meritevolezza di una determinata certificazione. Solo in questo modo si può, da un lato, garantire un monitoraggio efficace volto a circoscrivere i rischi di un uso abusivo ed elusivo di tale forma di impresa a danno dei consumatori, dei soci e di tutti i potenziali portatori di interessi e, dall'altro, conferire certezza ai limiti entro i quali gli amministratori non possono essere

22 Questo primo problema, come vedremo nel proseguo, è stato affrontato e risolto negli Stati Uniti mediante la previsione di un apposito sistema di certificazione esterna, accentrato in capo alla "*B-Lab*".

passibili di azioni di responsabilità per violazione dei propri doveri gestionali e fiduciari.

Oggi, l'esigenza di disporre di parametri univoci in sede di redazione del Report sull'impatto generato può essere soddisfatta grazie all'ingresso in Italia di uno strumento di valutazione largamente diffuso a livello globale, il c.d. "*B Impact Assesment*"[23] che, grazie al suo elevato livello di diffusione, potrebbe già consentire alle Società Benefit italiane di redigere la relazione annuale alla stregua di *standard* di valutazione uniformi.

3.2 Sistema di certificazione. Analizzando i vari aspetti maggiormente rilevanti di questa nuova forma di impresa, è stata più volte messa in evidenza l'esigenza di monitorare l'operato delle Società Benefit al fine di evitare che queste sfruttino indebitamente lo *status* per interessi commerciali e di immagine, senza rispettarne i requisiti di legge. Si potrebbe evitare tale inconveniente attraverso un processo di certificazione volto a rilasciare un attestato alla Società Benefit che, a fronte di puntuali controlli *ex ante* ed *ex post*, dimostri di essere in possesso dei requisiti previsti *ex lege*. In un certo senso, questo controllo si potrebbe paragonare a quello che il titolare di un marchio collettivo è obbligato ad effettuare nei confronti dei soggetti che richiedono l'adesione al marchio stesso, al fine di non incorrere in una decadenza del segno per uso decettivo. Trattasi di un controllo in entrata e di un controllo periodico successivo volto a garantire la conservazione delle caratteristiche essenziali affinché un imprenditore possa legittimamente beneficiare dei vantaggi derivanti dalla divulgazione di un messaggio di qualità e/o di provenienza sottostante al marchio collettivo.

23Il *B Impact Assessment* è uno strumento online gratuito che soddisfa i requisiti della legge sulle Società Benefit per la redazione del Report di Valutazione dell'Impatto o *Benefit Impact Report*. E' uno strumento di valutazione e un *benchmark* già utilizzato da oltre 50.000 imprese in 50 paesi per misurare, valutare, confrontare e migliorare le proprie performance economiche, sociali e ambientali. Si può generare un Report gratuito basato sulle risposte alle domande che misurano l'impatto su persone, comunità, clienti, altri *stakeholder* e ambiente. Il *B Impact Assessment* è disponibile in italiano (www.societàbenefit.net).

Mediante tale processo di certificazione, applicato nell'ambito in esame, si consentirebbe alle Società Benefit di dimostrare a terzi, quindi principalmente agli *stakeholders*, l'effettivo rispetto del messaggio di garanzia sotteso al "marchio", ovvero il perseguimento delle finalità sociali ed il raggiungimento delle *dual mission* statutariamente previste.

Tuttavia, in Italia, così come negli USA, non è stato previsto dal legislatore l'obbligo in capo alle Società Benefit di ottenere una specifica certificazione da parte di un soggetto terzo e indipendente[24].

Il carattere facoltativo del processo di certificazione ha quale *ratio* quella di evitare di aggravare le società con eccessivi costi e di rendere in tal modo ancora più impegnativa l'adozione di tale formula societaria.

Negli USA, l'esigenza di alcune società di conferire alla vesta di impresa in esame un effettivo valore ed ottenere dei concreti vantaggi in termini di immagine, ha determinato lo sviluppo di due tipi di *Benefit Corporation*: "ordinarie" e "certificate". In realtà, negli USA prima del riconoscimento giuridico delle *Benefit Corporation*, nel 2010 nasceva nel Maryland la cosiddetta "Certificazione *B-Corp*"[25], ovvero un *rating* volto a favorire la creazione di una "*community* di imprese" (CASTELLANI, DE ROSSI, RAMPA, 2016). In concreto, tale certificazione viene rilasciata dalla *B-Lab* alle imprese che decidono di sottoporsi ad una rigida selezione e che garantiscono un elevato livello di *performance* sociale ed ambientale. In tal modo, le società che potranno legittimamente fregiarsi del "marchio" di *Benefit Corporation*, conseguiranno un duplice risultato positivo: da un lato, consentiranno al consumatore ed alle diverse categorie di *stakeholders* di distinguere le aziende veramente virtuose da quelle che, diversamente, conducono un'attività di *marketing* ingannevole al

24 Il legislatore italiano si è, infatti, limitato a prevedere in termini generici la necessaria presenza di un ente avente la funzione di formulare standard di valutazione che le singole società dovranno adottare nella predisposizione della relazione annuale.

25 Tale certificazione viene rilasciata dalla "*B-Lab*", ente non-profit che ha quale oggetto sociale lo svolgimento di tre principali attività: 1) emissione di "marchi" - *Certified B-Corp* - ad imprese for-benefit; 2) sostegno e supporto per conferire un riconoscimento giuridico alle imprese for-benefit; 3) diffusione dello standard di valutazione aziendale concernente l'impatto e la creazione di valore socialmente utile, il cosiddetto "*Global Impact Investing Rating System* (GIIRS)".

solo fine di trarre i vantaggi commerciali derivanti dalla capacità attrattiva del marchio "*Certified B-Corp*"; dall'altro lato, potranno concretamente cogliere i frutti dell'investimento effettuato nella certificazione, giovandosi di un tangibile ritorno positivo in termini di immagine e di vantaggio concorrenziale sul mercato.

L'investimento nella certificazione *B-Corp* potrebbe essere equiparato ad un investimento in un "*intangible asset*", esattamente come se si trattasse di un marchio di impresa o collettivo dotato di capacità attrattiva e idoneità a comunicare verso l'esterno un messaggio di qualità e garanzia.

Tuttavia, anche tale certificazione non è di per sé sufficiente a garantire la conservazione nel medio-lungo termine degli effetti socio-ambientali positivi generati da una società. Infatti, la certificazione *B-Corp* è idonea ad attestare tali impatti positivi solo in un dato momento e non anche nel corso della vita di un'azienda. La forma giuridica della *Benfit Corporation*, invece, imponendo un determinato *imprinting* della *dual mission* prevista nell'oggetto sociale, conferirebbe attendibilità nel medio-lungo periodo. Certificazione *B-Corp* e *Benefit Corporation* sembrerebbero essere, pertanto, tra loro complementari.
Nonostante i limiti intrinseci propri di alcuni sistemi di controllo esterno, sarebbe auspicabile l'introduzione in Italia di un processo di certificazione sulla scia di quello statunitense. Questo potrebbe rappresentare uno strumento di fortificazione e valorizzazione del "marchio" di Società Benefit, di garanzia per gli *shareholders* e gli *stakeholders*, nonché di acquisizione di un maggior potere di mercato e, quindi, di competitività dell'impresa che decide di investire in un originale *intangible asset.*

4. La società benefit in Italia, oggi. Affrontati gli aspetti più caratterizzanti e problematici dell'istituto in esame, ad un anno e mezzo dal suo ingresso nel nostro ordinamento sembra opportuno analizzare i primi risultati da un punto di vista prettamente empirico. Pertanto, al fine di poter condurre un'analisi aggiornata delle Società Benefit, occorre focalizzarsi sul loro effettivo livello di diffusione in Italia. La possibilità di disporre di un quadro di questa

prima fase di “assestamento” della veste giuridica in esame consente inoltre di verificare quali degli effetti negativi ipotizzati al momento della sua introduzione si siano concretamente verificati e come potrebbero essere superati.

Al riguardo, si riportano di seguito i primi dati attestanti gli ambiti di diffusione e il grado di adesione da parte degli operatori economici italiani a tale veste giuridica, dal 1 gennaio 2016 ad oggi.

4.1 Dati empirici. I dati di seguito esposti si riferiscono, in particolare, alle Società Benefit iscritte nel Registro Ufficiale di B Lab[26], aggiornato al 08 agosto 2017, dal quale risulta che 105 società italiane hanno recepito e adottato tale veste giuridica.

4.2 Denominazione sociale. Per gli operatori economici che si avvalgono dello *status* di Società Benefit, ai sensi del comma 379 della Legge di stabilità 2016, è prevista la facoltà (“*La società benefit può*”), e non l'obbligo, di riportare accanto alla denominazione o ragione sociale le parole “Società benefit” o la relativa sigla “SB”, nonché di utilizzare le medesime “*nei titoli emessi, nella documentazione e nelle comunicazioni verso i terzi”.* A primo impatto potrebbe sembrare superflua come previsione. Dovrebbe essere, infatti, interesse della stessa società comunicare all'esterno la propria veste, soprattutto alla luce degli sforzi, economici e non, dalla stessa sostenuti per potersi avvalere di tale modello e della capacità attrattiva che l'integrazione della denominazione sociale di cui sopra potrebbe esercitare sul pubblico dei consumatori. Inoltre, trattandosi di un'informazione delicata e rilevante per le scelte dei creditori e degli investitori, sarebbe forse stato più opportuno, per soddisfare esigenze di trasparenza, imporre, e non presentare come facoltativa, tale integrazione della denominazione sociale. Così, infatti, è previsto in gran parte degli Stati Uniti d'America, dove le legislazioni dei singoli Stati[27] prevedono l'obbligo per le

26 Dati raccolti dal Registro Ufficiale delle Società Benefit italiane curato da B Lab e pubblicato sul sito ufficiale www.societàbenefit.net.

27 Particolare, anche su questo fronte, è la legge del Delaware, la quale non impone l'utilizzo di particolari formule nella denominazione sociale, ma obbliga le società, che emettono azioni o

Benefit Corporation di introdurre nella propria denominazione sociale le parole "*general benefit corporation*" (o la sigla "GBC") oppure "s*pecific benefit corporation*" (o "SBC")[28].

Pertanto, alla luce delle considerazioni di cui sopra, l'inserimento della dicitura "Società *benefit*" nella denominazione sociale rappresenta uno degli strumenti principali per divulgare l'acquisizione della qualifica *benefit* e per trarne i vantaggi in termini di reputazione ed immagine. Per tale motivo ben si comprende la tendenza di quasi tutte le Società Benefit italiane di riportare nella propria denominazione sociale una delle summenzionate diciture. Infatti, su 105 società che si sono statutariamente obbligate a perseguire una o più *dual mission*, 103 hanno inserito nella propria denominazione sociale una delle espressioni di cui sopra. Le uniche due società che, allo stato attuale, hanno omesso tale indicazione sono rispettivamente una S.p.A., operativa nel settore di cura ed assistenza sanitaria, e una S.r.l., attiva nel settore enogastronomico (organizzazione di manifestazioni, vendita per corrispondenza prodotti enogastronomici e commercio elettronico di eventi su prenotazione).

4.3 Tipologie di società. Con riferimento alle tipologie di società abilitate ad avvalersi della veste giuridica di Società Benefit, al comma 377 della Legge di Stabilità 2016, il legislatore ha consentito il perseguimento dello scopo di beneficio comune a tutte le società di cui al libro V, titoli V e VI del codice civile. Pertanto, la qualifica di Società Benefit può essere legittimamente acquisita dalle società di persone, dalla società di capitali e dalle cooperative nel rispetto

titoli partecipativi, ad informare con le modalità più opportune i soggetti interessati. Delaware Code, Title 8, Corporations, Chapter 1. General Corporation Law, Subchapter XV, Public Benefit Corporation, § 362 Public benefit corporation defined; contents of certificate of incorporation. «(c) The name of the public benefit corporation may contain the words 'public benefit corporation' or the abbreviation 'P.B.C.' or the designation 'PBC' which shall be deemed to satisfy the requirements of § 102(a)(l)(i) of this title". § 364 Stock certificates; notices regarding uncertificated stock. "Any stock certificate issued by a public benefit corporation shall note conspicuously that the corporation is a public benefit corporation formed pursuant to this subchapter.».

28 Minnesota Statute, 304A.101 Subd. 2. «*Name requirements. A public benefit corporation name must comply with the requirements of section 302A.115 other than subdivision 1, paragraph (b), and with respect to: (1) a general benefit corporation, contain the words "general benefit corporation," or the abbreviation "GBC;" and (2) a specific benefit corporation, contain the words "specific benefit corporation," or the abbreviation "SBC."».*

della relativa disciplina.

Su un totale di 105 Società Benefit attualmente risultanti dal relativo registro ufficiale, si può notare una netta prevalenza di società a responsabilità limitata, in particolare 93 società, di cui 4 nella forma di s.r.l. semplificate e 3 di *start up* innovative. Un'analoga tendenza non può ancora riscontrarsi tra le società per azioni che, sebbene in lieve aumento, sono appena 7. Tra queste, la consolidata azienda "Antica Erboristeria", la "E. DI. C." e la "LifeGate", entrambe solide realtà dotate di un consistente capitale sociale. Solo 4 le società cooperative e un unico esponente, rispettivamente, per le società di persone (s.n.c.) e per le società semplici tra professionisti.

4.4 Distribuzione territoriale. Occorre, altresì, verificare in quali aree territoriali della penisola italiana si sono maggiormente diffuse le Società Benefit. Prendendo come riferimento la tradizionale tripartizione: nell'Italia Settentrionale, dove è ravvisabile la maggior concentrazione, sono 72 gli operatori economici che si sono avvicinati alla nuova vesta giuridica; nell'Italia Centrale sono 22 e, infine, nell'Italia Meridionale (e nelle Isole) si assiste ad un notevole ridimensionamento del livello di diffusione, essendo appena 11 le società che si fregiano dello *status* di Società Benefit.

4.5 Aree di attività. Aderendo ad una interpretazione autentica del nuovo istituto, si può addivenire alla conclusione che le Società Benefit interiorizzano e amalgamano la finalità di beneficio comune con un'attività economica imprenditoriale volta alla massimizzazione del profitto. Dall'elenco delle Società Benefit attualmente registrate in Italia risulta che esse operano in settori complessivamente eterogenei, sebbene vi siano delle aree di attività caratterizzate da una maggior concentrazione. In particolare, si riscontra una preponderante tendenza ad adottare lo *status* di SB nel settore dei servizi in generale e, più in particolare, dei servizi di natura informatica, dove risultano registrate ben 22 società. A seguire, i settori nei quali si ravvisa un maggior livello di adesione sono quello sanitario, unitamente al complementare settore

dei beni e servizi per la cura della persona, dove si annoverano 15 società aderenti; il settore concernente l'attività di assistenza a soggetti deboli e la formazione scolastica, con 13 società registrate; il settore alimentare e della ristorazione, con 9 esponenti. Infine, nei restanti settori (quali abbigliamento, turismo, immobiliare, editoria, agricoltura, ricerca e sviluppo, ambiente, consulenza finanziaria, energia) oscillano tra un numero di 2 e 7 le società che hanno aderito alla nuova veste di impresa.

4.6 Oggetto sociale: *dual mission* e attività d'impresa. In merito all'oggetto sociale delle Società Benefit sin qui analizzate occorre mettere in luce due aspetti in particolare: *i)* il tipo e il grado di specificità con i quali una o più finalità di beneficio comune vengono statutariamente indicate, *ii)* la sussistenza o meno di un legame tra l'attività di impresa e la *dual mission*.

Trattasi di due aspetti dirimenti in quanto dagli stessi, per i motivi sovraesposti, si potrebbe già rinvenire la presenza di margini per un uso abusivo dello *status* di Società Benefit.

Con riferimento al primo aspetto, ed in particolare al grado di determinatezza della finalità di beneficio comune che la società si impegna a perseguire, si riscontra una tendenza complessivamente eterogenea. Infatti, la *dual mission* viene individuata, a seconda dei casi, con *a)* formule molto generiche, quali «*La società, oltre allo scopo di dividerne gli utili, persegue una o più finalità di beneficio comune e opera in modo responsabile, sostenibile e trasparente nei confronti di persone, comunità, territori e ambiente, beni ed attività culturali e sociali, enti e associazioni ed altri portatori di interesse.»,* che, per l'eccessiva indeterminatezza, sembrerebbero porsi in contrasto con le disposizioni normative; *b)* una pluralità di scopi di beneficio comune dettagliatamente descritti e tra loro omogenei (in termini di beneficiari e/o di aree di attività coinvolte), come se fossero più facce della stessa medaglia; *c)* singole finalità altruistiche a vantaggio di categorie indeterminate di soggetti (es. "persone", "collettività") o della natura e dell'ambiente in generale o dell'attività di ricerca e sviluppo; *d)* benefici e/o minor danni per determinate

categorie di beneficiari (es. “consumatori”, “imprenditori”, “extracomunitari”, “minori”, “lavoratori”, etc.) che consentono di restringere l’ambito della *dual mission* perseguita.

Quanto al tipo di finalità di beneficio comune, si riscontra una generale eterogeneità degli scopi altruistici perseguiti. Si registra, tuttavia, una prevalenza di *dual mission* rivolte a favorire la tutela dell’ambiente, sia in termini di interventi attivi, *i.e*. «*la promozione (presso gli stessi utenti e tramite analoghi canali) di azioni con impatto sociale positivo*», sia in termini di minor danni mediante l’adozione di materiali e/o tecniche d’impresa ecosostenibili*, i.e. «la promozione presso i propri utenti (e quindi la cittadinanza) di comportamenti a basso impatto ambientale (rispetto ad alternative più inquinanti) attraverso i propri applicativi e canali di comunicazione*; *la promozione esclusiva (presso gli stessi utenti e tramite analoghi canali) di prodotti e servizi legati ad un consumo etico ed eco-sostenibile*». Tra le altre finalità di beneficio comune si possono individuare investimenti nella ricerca e nello sviluppo, misure di tutela e di coinvolgimento dei lavoratori (*i.e.* «*attraverso l’attuazione di politiche dirette a garantire una partecipazione dei lavoratori alla gestione societaria […]; consentire ai lavoratori opportunità di crescita professionale e umana mediante la promozione, anche nel contesto aziendale, di iniziative dirette a migliorare la qualità dell’ambiente di lavoro*»), valorizzazione di particolari aree o città italiane (*i.e.* «*la valorizzazione e la promozione della città di Venezia e della sua laguna e della sua storia e cultura*»).

Con riferimento al secondo aspetto, ovvero alla sussistenza di una continuità tra l’attività di impresa e la *dual mission,* spesso è possibile riscontrare una certa coerenza tra le due attività.

Ad esempio, in alcuni casi, beneficiari della finalità altruistica sono proprio i dipendenti della stessa società che si è statutariamente obbligata a perseguirla. In altri casi, i beni e servizi offerti vengono realizzati mediante impianti e sistemi di produzione ecosostenibili, quindi il beneficio comune viene direttamente “interiorizzato” nelle tecniche di produzione. In altri casi ancora si assiste ad una commistione tra le due finalità, altruistiche e lucrative; infatti, alcune società

mirano a realizzare ed erogare prodotti che per le loro caratteristiche intrinseche sono idonei a ottimizzare le risorse disponibili e a garantire un conseguente risparmio energetico («*la società si impegna altresì a coniugare tecnologia ed ecologia (green computing), puntando alla minimizzazione ed efficientamento delle risorse hardware da impiegare, con conseguente risparmio energetico e diminuzione di rifiuti informatici*.»).

4.7 Prime riflessioni. Alla luce delle attuali risultanze empiriche si possono fare alcune riflessioni, in questa fase non più meramente ipotetiche, bensì corroborate da dati.

In particolare, con riferimento alla *denominazione sociale* risulta una generale tendenza delle società ad optare spontaneamente, mediante l'introduzione della dicitura "Società benefit/SB" nella propria denominazione sociale, per la trasparenza e la divulgazione verso l'esterno del loro impegno a perseguire uno scopo di beneficio comune. Tale tendenza potrebbe interpretarsi quale indice della consapevolezza delle società che hanno adottato la veste giuridica di Società Benefit della capacità attrattiva di tale veste e dell'importanza di presentarsi sul mercato come società attive e sensibili alle tematiche ambientali e/o economico-sociali oggetto della *dual mission*. È, altresì, interessante notare come vi siano alcune Società Benefit italiane munite della certificazione americana di "*B-Corp*"; certificazione, lo ricordiamo, che avvalora e garantisce l'effettività dell'impegno altruistico assunto dalle società che dimostrano di disporre di elevati livelli di *performance* ambientale e sociale.

Per quanto concerne le *tipologie* di società italiane che hanno adottato la veste di Società Benefit, nel primo anno e mezzo di applicazione si registra una prevalenza di società di capitali ed in particolare di S.r.l.. Tra le S.r.l. va evidenziata la presenza delle varianti di S.r.l.s. e di *Start up* innovative. Inoltre, si riscontra positivamente un lieve aumento delle S.p.A., nonché la costituzione di n. 4 società cooperative *benefit*. Da questi dati si può, pertanto, evincere una

maggior sensibilità delle società di minore dimensione per le finalità altruistiche indicate nella Legge di Stabilità 2016.

Quanto alla *distribuzione* delle Società Benefit *sul territorio* italiano, si riscontra una netta prevalenza nelle regioni dell'Italia settentrionale. Tale circostanza probabilmente prescinde dalle caratteristiche intrinseche dell'istituto in esame, mentre sembrerebbe riflettere la già nota maggior concentrazione delle attività imprenditoriali nel nord del nostro paese.

Quanto ai *settori di attività* interessati, dall'analisi empirica risulta che le Società Benefit operano in settori abbastanza eterogenei; è, tuttavia, possibile riscontrare una notevole prevalenza nel settore informatico, sanitario e assistenziale. Le aree di attività nelle quali complessivamente operano tali società riflettono, in modo più o meno intenso, la loro propensione a bilanciare il perseguimento della massimizzazione del profitto con la volontà di apportare un beneficio a determinate categorie di soggetti in termini di miglioramenti, vantaggi e/o minor danni all'ambiente, all'economia nazionale, alla collettività dei consociati o a categorie determinate di soggetti (quali bambini, extracomunitari, utenti di associazioni di categoria, imprenditori, etc.). Trattasi, infatti, di settori e di aree di attività di interesse prevalentemente generale, caratterizzati da un forte risvolto altruistico. Infine, in merito all'*oggetto sociale* e all'individuazione nello stesso della *dual mission* e dell'attività di impresa, si riscontra una notevole eterogeneità da un punto di vista delle finalità statutariamente previste. Le *dual mission* solo in alcuni casi sono individuate in termini piuttosto generici; nella maggior parte dei casi le singole finalità che la società intende perseguire sono descritte nel dettaglio, mentre le modalità e i mezzi per il raggiungimento di tali scopi risultano a volte indeterminati o troppo generici. Quanto al legame e alla sussistenza di un rapporto di continuità tra le finalità altruistiche statutariamente previste e la principale attività economica di ciascuna Società Benefit, sebbene non sussista alcun obbligo esplicito in tal senso, sembrerebbe riscontrarsi una virtuosa tendenza delle società, in linea con la volontà originaria ed implicita del legislatore, a perseguire una o più *dual mission* coerenti con l'attività di impresa effettivamente svolta. Come è stato già

detto, tale vicinanza tra gli oggetti delle finalità della Società Benefit è indice di una maggior serietà dell'impegno altruistico assunto, essendo più credibile che una società già operativa in un determinato settore possa impegnarsi ad apportare dei benefici o ridurre le esternalità negative proprio sul settore in cui opera.

5. Considerazioni conclusive. Volendo a questo punto trarre delle preliminari conclusioni sull'argomento trattato, il modello di impresa analizzato in questa sede può essere sicuramente considerato il risultato di un progetto ambizioso e propositivo. Tuttavia, proprio in quanto frutto di un nuovo paradigma economico e imprenditoriale, non si possono ignorare alcune criticità emerse alla luce di una prima analisi prettamente astratta e ipotetica. Si è manifestata sin da subito l'opportunità di introdurre degli accorgimenti idonei a garantire il mantenimento e l'effettivo perseguimento della *dual mission* a tutela dalle categorie degli *stakeholders* e *shareholders*, nonché dei consumatori. Pertanto, nonostante la previsione di ulteriori obblighi di trasparenza e rendicontazione in capo agli amministratori, è stata immediatamente messa in luce la necessità di rendere effettivo e sul merito il controllo affidato all'Autorità Garante della concorrenza e del mercato nei casi, ad esempio, di pubblicità ingannevole (v. Relazione accompagnatoria al disegno di legge n.1882).

È, altresì, emersa la necessità di rendere accessibili, a chi ha il potere di esercitare un'attività di vigilanza, mezzi e modalità idonee di pubblicizzazione sia della natura ibrida della società che della relazione annuale degli amministratori; ciò al fine di poter fornire sia al pubblico dei consumatori, sia agli *stakeholders* che agli *shareholders* di una Società Benefit gli elementi su cui svolgere un monitoraggio.

Sempre in termini di controllo volto ad evitare un uso abusivo del 'marchio' "Società Benefit", la società, i soci e i consumatori o, più in generale, tutti gli altri portatori di interessi, dovrebbero poter agire nei confronti degli amministratori avvalendosi delle azioni di responsabilità codicistiche.

Inoltre, poiché il controllo sul *self-commitment* di una Società Benefit si basa sulla relazione annuale redatta dall'organo gestorio alla stregua di uno dei possibili *standard* di valutazione, l'assenza di un unico *standard* di riferimento e di un unico *standard setter* (come è invece la *B-Lab* statunitense) determina una pericolosa frammentarietà che potrebbe indebolire la possibilità di esercitare un controllo efficace sull'operato della società. È, quindi, essenziale favorire la diffusione di un sistema di certificazione, sulla scia del modello statunitense, che preveda univocità e uniformità sia degli *standard setter* che di valutazione; si potrebbe inoltre prevedere un efficace controllo *ex ante* ed *ex post* sull'effettivo possesso dei requisiti richiesti nei confronti delle società che intendono avvalersi del marchio "Società Benefit" nella propria denominazione o ragione sociale, come avviene in un procedimento di adesione ad un marchio collettivo.

Inoltre, per garantire anche ai soci di una Società Benefit la continuità nel perseguimento della *dual mission*, sarebbe forse opportuno introdurre *quorum* deliberativi e costitutivi qualificati per poter eliminare, sostituire o modificare lo scopo di beneficio comune statutariamente previsto. Infatti, l'applicazione della disciplina ordinaria prevista per le singole forme societarie comporta la possibilità per i soci di apportare delle modifiche allo statuto e conseguentemente alla *dual mission* in esso prevista, senza dover rispettare particolari maggioranze qualificate.

Al fine di garantire una maggior diffusione della forma di impresa in esame, sulla base di una prima valutazione "istintiva" si potrebbe caldeggiare l'opportunità di compensare i sacrifici e i maggiori oneri (sia economici che gestionali) "sopportati" da una Società Benefit con incentivi fiscali idonei ad attenuare le difficoltà che quest'ultima potrebbe ragionevolmente dover/voler affrontare nei suoi primi anni di vita, ovvero prima che il potenziale – e forse implicitamente auspicato – ritorno in termini di immagine e reputazione possa concretamente tradursi in un ritorno anche di natura economica o quantomeno monetizzabile. Tuttavia la previsione di finanziamenti ed agevolazioni fiscali potrebbe avere un effetto *boomerang*, snaturando di fatto l'istituto stesso e

innescando meccanismi tutt'altro che virtuosi da parte delle imprese, le quali finirebbero per adottare la filosofia e la veste delle Società Benefit al solo scopo di ottenere vantaggi di natura fiscale.

È innegabile che le suesposte difficoltà potrebbero in parte disincentivare la diffusione di tale forma di impresa. Vi sono numerosi ostacoli e ciò è insito nell'adozione di un modello in linea con un innovativo paradigma economico che richiede più sacrifici nel breve termine, a fronte di vantaggi nel medio/lungo periodo; vantaggi, questi ultimi, diretti e messi a disposizione della collettività e non unicamente e necessariamente a coloro che, mediante i propri conferimenti, hanno sostenuto il rischio di impresa.

Alla luce dei recenti sviluppi si può ritenere che parte delle paure e delle criticità sorte al momento dell'introduzione delle Società Benefit siano venute meno o, comunque, si siano ridimensionate.

In primo luogo, la prassi sembrerebbe aver già in parte colmato la lacuna normativa relativa alla mancata previsione di un unico *standard* di valutazione e di un unico *standard setter*. Oggi, l'esigenza di disporre di parametri univoci in sede di redazione del *Report* sull'impatto generato può essere soddisfatta grazie all'ingresso in Italia di uno strumento di valutazione largamente diffuso a livello globale, il c.d. "*B Impact Assesment*"[29] che, per il suo elevato livello di diffusione, potrebbe già consentire alle Società Benefit italiane di redigere la relazione annuale alla stregua di *standard* di valutazione uniformi.

In secondo luogo, la generale tendenza delle società a individuare statutariamente *dual mission* dettagliate e coerenti con la propria attività economica imprenditoriale può attenuare il timore di un uso abusivo e distorto della veste giuridica in esame, spesso derivante da indicazioni meramente generiche e di facciata delle finalità di beneficio comune.

29 Il *B Impact Assessment* è uno strumento online gratuito che soddisfa i requisiti della legge sulle Società Benefit per la redazione del *Report* di Valutazione dell'Impatto o *Benefit Impact Report*. E' uno strumento di valutazione e un *benchmark* già utilizzato da oltre 50.000 imprese in 50 paesi per misurare, valutare, confrontare e migliorare le proprie *performance* economiche, sociali e ambientali. Si può generare un *Report* gratuito basato sulle risposte alle domande che misurano l'impatto su persone, comunità, clienti, altri *stakeholder* e ambiente. Il *B Impact Assessment* è disponibile in italiano (www.societàbenefit.net).

Infine, dalla diffusa tendenza a inserire la dicitura “Società benefit” nella denominazione sociale non si può non ravvisare una certa fiducia e serietà dell’investimento nello *status*. Da questo indirizzo si può infatti dedurre una maggior serietà delle società italiane, almeno nella fase di partenza, a impegnarsi in modo trasparente verso l’esterno. La maggior divulgazione e trasparenza, da una parte, incrementa le possibilità per tali società di conseguire tutti i vantaggi a cui si è già accennato in termini di immagine e di reputazione, dall’altra, le espone inevitabilmente ad un maggior controllo e a maggiori pretese da parte dei beneficiari della finalità statutariamente prevista. Si pongono, in altre parole, sotto i riflettori delle varie categorie di portatori di interessi i quali saranno più inclini a voler vedere soddisfatte le proprie aspettative.

Che vi siano delle difficoltà applicative è innegabile. Tuttavia, dove ci sono cambiamenti ci sono quasi sempre nuove sfide e difficoltà. Difficoltà che potranno essere superate attraverso un’evoluzione normativa e un’interpretazione delle norme attuali idonee a garantire un’equilibrata e incentivante allocazione delle risorse. Risorse risultanti dall'esercizio di un'attività di impresa che tenta coraggiosamente, ma con notevole lungimiranza, di creare complementarietà e sinergia tra il perseguimento di finalità aventi nature diverse, ma non per questo incompatibili.

Non si può ancora dire con certezza se la Società Benefit riscontrerà successo o meno e se assisteremo ad un incremento numerico delle stesse. Si può, tuttavia, avere fiducia nel “nuovo” e assistere al suo naturale sviluppo con la consapevolezza che *«non sempre cambiare equivale a migliorare, ma per migliorare bisogna cambiare*[30]».

30 Winston Leonard Spencer Churchill (1874-1965).

Riferimenti bibliografici

ASSONIME – Associazione fra le società italiane per azioni, *La disciplina delle società benefit*, in Circolare n.19 del 20 giugno 2016, Diritto Societario, 2016
BORGIA F., *Responsabilità sociale di impresa e diritto internazionale: tra opportunità ed effettività,* Ianus, 2010
BUONOCORE V. - CAPO G., *Manuale di diritto commerciale,* Giappichelli, 2016
CAMPOBASSO G.F. - CAMPOBASSO M., *Diritto commerciale. Vol. II: Diritto delle società,* 2015
CASTELLANI G. - DE ROSSI D. - RAMPA A., Fondazione Nazionale dei Commercialisti, *Le Società Benefit. La nuova prospettiva di una social corporate responsibility con Commitment,* 2016
COCIOLILLO M., *Scelte gestorie e finalità di beneficio comune nel nuovo modello di società benefit,* in *LUISS Law Review n.1/2017,* 2017
CONTE G., *Codici etici e attività di impresa nel nuovo spazio globale di mercato*, in *Contr.Impr*.,131, 2006
CUMMINGS B. *Benefit Corporations:how to enforce a mandate to promote the public interest*, in *Columbia Law Review*, 2012
GALLI C., *Il marchio*, in *Il diritto, Enc. Giur.*, IX, Milano, 2007
GALLI C. (a cura di), *Codice della proprietà industriale: la riforma 2010*, Ipsoa, 2010
GALLI C., *Segni distintivi e denominazione d'origine:* l*a tutela della comunicazione d'impresa e la generalizzazione della protezione contro il parassitismo*, in *La revisione del Codice della Proprietà Industriale: da un'impostazione "proprietaria" a un approccio market oriented,* 2011
HILLER J.S., T*he Benefit Corporation and Corporate Social Responsibility,* in *Journal of Business Ethics,* 2013
McDONNEL B.H., *Committing to doing good and doing well: fiduciary duty in Benefit Corporation*, in *Un. Minn. Legal Studies Research Paper Series*, n.14-21, 2014
MOSCO G.D., *L'impresa non speculativa*, in *Giurisprudenza Commerciale,* Anno XLIV Fasc. 2-2017
PAGAMICI B., *Società 'benefit': sintesi tra imprese 'for profit' e 'non profit',* in *Cooperative e Enti non profit,* n.4, 2016
RACUGNO G., *L'impresa sociale*, in *Rivista di diritto commerciale,* n.49, 2009
RIOLFO G., *Le società benefit in Italia: prime riflessioni su una recente innovazione legislativa*, in *Attualità e saggi*, *Studium Iuris* n.6/2016
VANZETTI A. - DI CATALDO V., *Manuale di diritto industriale,* 6° edizione, Milano, 2009

Atti e provvedimenti

Italia
Legge n.208 del 28 dicembre 2015, *Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato* ("legge di stabilita' 2016")
Decreto Legislativo n. 155 del 24 marzo 2006, *Disciplina dell'impresa sociale, a norma della Legge 13 giugno 2005 n. 118*, pubblicato nella Gazzetta Ufficiale n. 97 del 27 aprile 2006
Decreto Legislativo n. 74 del 25 gennaio 1992 *in materia di pubblicità ingannevole e comparativa*
Decreto Legislativo 10 febbraio 2005, n.30, *Codice della Proprietà Industriale*, *a norma dell'articolo 15 della legge 12 dicembre 2002, n. 273*
Relazione accompagnatoria al disegno di legge n.1882 presentato al Senato nell'aprile del 2015 e trasfuso nella Legge di Stabilità 2016
Unione Europea
Commissione delle Comunità Europee, Libro Verde, *Promuovere un quadro europeo per la responsabilità sociale delle imprese* (COM) 2001.
Stati Uniti
Minnesota Statute, 304A.101 Subd. 2
Delaware Code, Title 8, Corporations, Chapter 1

Giurisprudenza
Italia
Tribunale di Firenze del 29 maggio 2015, Sez. Spec. Impresa, *Ilsocietario.it,* 2015, 24 agosto
Stati Uniti
Corte Suprema del Michigan, n. 170 NW 668, *Dodge - Ford Motor Company,* 1919

Parte seconda

Dossier monografico
Cyber Security, Digital Privacy & Artificial Intelligence

Presentazione

Luiss Law Review inizia con questo numero la pubblicazione di sezioni monografiche dedicate a temi di particolare rilievo da approfondire con prospettive e su aspetti diversi.

L'inserimento di una parte monografica non esclude in genere, come in questo numero, la presenza di altri contributi, così da lasciare spazio anche a sollecitazioni e analisi su argomenti diversi.

Questo primo dossier è dedicato a due materie oggi fondamentali, vicine e spesso interconnesse: la sicurezza informatica e la protezione della *Privacy* digitale nell'epoca, ormai a tutti gli effetti iniziata, dell'intelligenza artificiale.

Gran parte dei contributi trovano origine nel dottorato Diritto e Impresa del Dipartimento di Giurisprudenza Luiss Guido Carli diretto da Giuseppe Melis, grazie soprattutto all'impegno e alla passione di Riccardo Piselli, dottorando del XXXII ciclo.

Con riguardo alla Cyber Security, è indispensabile per il nostro Paese poter contare su una pubblica amministrazione consapevole delle minacce informatiche e in grado di difendersi adeguatamente. Come sottolinea il contributo di Marta Zilianti, negli ultimi anni sono stati fatti passi avanti importanti in questa direzione nonostante la limitatezza delle risorse economiche disponibili, che ne rappresenta forse il principale ostacolo. Si è in particolare proceduto a una nuova organizzazione della nostra struttura istituzionale di sicurezza informatica, rafforzando il coordinamento degli interventi di prevenzione, protezione e gestione affidato al CISR (Comitato interministeriale per la sicurezza della Repubblica) e al DIS (Dipartimento per l'informazione per la sicurezza).

Sul fronte delle imprese, specie minori, per elevare il livello di sicurezza informatica è auspicabile ricorrere anche a strumenti di collaborazione imprenditoriale quali il consorzio o il contratto di rete, ferma la necessità di un intervento anzi tutto pubblico in tema di *Information Sharing*, secondo le previsioni della Direttiva NIS. Strumenti che possono consentire di contenere i costi e di mettere in moto il percorso virtuoso ipotizzato dal Rapporto 2016 del

CIS e del Laboratorio nazionale di Cybersecurity, come osserva Gian Domenico Mosco. Possono contribuire anche strumenti agevolativi di carattere fiscale, pur di portata più ampia, come il c.d. iperammortamento esaminato nel contributo di Alessandro Liotta.

Problemi di sicurezza informatica e di protezione dei dati personali emergono anche quando si ricorre per la conclusione dei contratti e in genere per la sottoscrizione di documenti alla firma grafometrica, che consiste in una sottoscrizione elettronica ma olografa apposta su un tablet o su altri dispositivi, che possono rilevare anche dati biometrici identificativi del sottoscrittore quali la pressione o la velocità di tracciamento. Mentre già si intravedono gli ancora più ampi rischi della diffusione per l'identificazione di una persona della biometria fisica (iride, impronta digitale, volto, ecc.) o dei microchips sottopelle (secondo il *Wall Street Yournal,* già utilizzati nel mondo da non meno di 30.000 persone), emerge la necessità, messa in luce dal contributo di Maria Rosaria Lenti, di una forte attenzione verso il fenomeno, pur regolato da un provvedimento del 2014 dell'Autorità garante per la protezione dei dati personali, così da rendere più efficaci le misure di prevenzione e da poter reagire prontamente a minacce oggi ancora sconosciute o sottovalutate, ma probabili considerati la complessità del mondo digitale e lo sviluppo ancora iniziale dello strumento.

È inutile sottolineare l'importanza del diritto penale con riguardo alla Cyber Security, pur se attualmente non esiste una regolamentazione penalistica specifica della materia. Nel contributo di Luca D'Agostino si osserva però che il recepimento della direttiva NIS - 2016/1148 UE e in parte le stesse fonti di auto-regolamentazione comporteranno, almeno per i fornitori di servizi essenziali o di servizi digitali, obblighi di *compliance* e una conseguente responsabilità in caso di mancata o insufficiente adozione di misure adeguate di prevenzione e protezione o di violazione degli obblighi di notifica, con un presumibile rafforzamento dei presidi organizzativi per la sicurezza informatica.

A livello europeo, è l'ENISA, l'Agenzia Europea per la sicurezza delle reti e dell'informazione creata nel 2004, a occuparsi della materia: il contributo di

Elena Pauri ricostruisce l'attuale quadro normativo ed esamina le prospettive di riforma dell'Agenzia.

Vantaggi e pericoli dell'intelligenza artificiale, e dei Big Data che ne sono alla base, sono divenuti oggetto di dibattito anche non specialistico via via che se ne è toccata con mano la diffusione nella vita di tutti i giorni, una diffusione senza dubbio destinata a incrementarsi fortemente, ma con contenuti (se e quando la I.A. assomiglierà a quella umana?) oggi non prevedibili sulla base delle tecnologie disponibili. Come si sta cercando di governare l'Intelligenza Artificiale e cosa andrà fatto in futuro è indicato nella ricca ricognizione di Tulio Rosembuj.

Uno dei problemi più rilevanti suscitati dall'I.A. è senza dubbio la tutela della *Privacy,* ormai vista essenzialmente come protezione dei dati personali.

Non è un caso che il Regolamento (UE) 2016/679 in materia di protezione di dati personali preveda che dal 25 maggio 2018 vi siano limiti al trattamento dei dati personali che avvenga sulla base di un processo decisionale "automatizzato" e che, se il trattamento è consentito, l'interessato abbia almeno il diritto di ottenere l'intervento umano del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. Altrettanto significativo è che chiunque di noi abbia dal prossimo maggio il c.d. "diritto alla spiegazione", vale a dire il diritto di ricevere "informazioni significative", tra l'altro, sulla "logica utilizzata" dall'algoritmo.

Riccardo Piselli si interroga però sui limiti del regolamento 2016/679 di fronte allo sviluppo degli algoritmi di *deep learning* e sulla *privacy* come strumento che ormai si affianca al diritto *antitrust* nella regolamentazione della competizione imprenditoriale, mentre il diritto alla portabilità dei dati anche come fattore pro-concorrenziale è esaminato nel contributo di Andrea Giulia Monteleone.

Infine, Ernani Francesco Cesareo si occupa dell'introduzione da parte dell'art. 24 del regolamento (UE) 2016/679 del principio di *Accountability,* che chiama il responsabile del trattamento a mettere in atto misure tecniche e

organizzative adeguate per garantire che il trattamento sia realizzato nel rispetto del regolamento e a poterlo dimostrare.

L'importanza e la complessità dei problemi suscitati dall'Intelligenza Artificiale è testimoniata dall'approvazione da parte del Parlamento europeo il 16 febbraio 2017 di una risoluzione che raccomanda alla Commissione di predisporre una regolamentazione civilistica della robotica e di valutare l'opportunità di istituire un'Agenzia europea per la robotica e l'intelligenza artificiale. Avremo presto una direttiva europea in materia, speriamo organica e ben meditata?

Sezione Prima: Cyber Security

Verso un'architettura digitale unica e sicura per la P.A.: il ruolo di AgID e Consip

Di **MARTA ZILIANTI**

SOMMARIO: – **1.** INTRODUZIONE. – **2.** AGID E CONSIP: DUE FACCE DELLA STESSA MEDAGLIA. – **3.** VERSO UN'ARCHITETTURA ISTITUZIONALE DI SICUREZZA CIBERNETICA. – **4.** POSSIBILI CRITICITA' E CONSIDERAZIONI CONCLUSIVE.

Abstract

This paper presentation explores the development of the new relationship between the public administration and the cyber security in light of the defense of the IT heritage, taking into consideration the key role of AgID and Consip and the complex architecture of cyber security to be implemented by the public entities following the AgID resolutions and the rules adopted during the last few years.

1. Introduzione. Non si ravvisa una normativa copiosa circa il rapporto tra pubblica amministrazione e cyber security. Le prime fonti si individuano infatti nel Codice dell'amministrazione digitale[1] e, ancora prima, nel Codice in materia di protezione dei dati personali[2]. Successivamente, il tema in questione è stato preso in esame dal legislatore con il Decreto Sviluppo del 2012[3] e il Decreto Crescita del medesimo anno[4], fino a giungere al d.p.c.m. del 24 gennaio 2013 recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, abrogato recentemente da un analogo decreto che si esaminerà nel prosieguo.

La disciplina normativa, inizialmente scarna, quindi si è evoluta nel tempo. L'art. 51 del Codice dell'amministrazione digitale sopra citato ha introdotto delle regole di sicurezza dei dati, dei sistemi e delle infrastrutture

1 Art. 51 del d.lgs. 7 marzo 2005, n. 82.
2 Allegato B, Disciplinare tecnico in materia di misure minime di sicurezza del d.lgs. 30 giugno 2003, n. 196.
3 Art. 20, comma 3, lett. b), del d.l. 22 giugno 2012, n. 83, convertito con modificazioni dalla l. 7 agosto 2012, n. 134, concernente misure urgenti per la crescita del Paese.
4 Art. 33-septies del d.l. 18 ottobre 2012, n. 179, convertito in l. 17 dicembre 2012, n. 221, recante ulteriori misure urgenti per la crescita del Paese.

delle pubbliche amministrazioni. In particolare, sono state adottate soluzioni tecniche per la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati detenuti dalla P.A.. L'art. 51, comma 2, stabilisce in proposito che «I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta».

Il rischio cyber nei sistemi informatici delle P.A. è esploso negli ultimi anni, grazie all'esigenza di superare le criticità sorte con lo sviluppo tecnologico e per porre fine alle insidie alla sicurezza informatica[5]. In particolare, le amministrazioni possono essere facilmente esposte ad una serie di pericoli quali, la sottrazione, l'alterazione o la distruzione delle informazioni dalle stesse conservate. I servizi delle P.A. possono essere degradati, alterati o bloccati e le fonti possono essere confuse o alterate, inoltre, possono subire alterazioni le autorizzazioni o essere manomessi o distrutti i sistemi di controllo e di monitoraggio dalle stesse utilizzate.

Tali insidie avvengono tramite strumenti quali il contagio da malware (virus, botnet, phishing) o attacchi cibernetici (cybercrime, cyber war, activisms). Molto comuni sono anche il furto di credenziali o di identità, mediante la personificazione di un soggetto, una organizzazione o un servizio e il degrado, l'interruzione o la distruzione di un servizio.

Ne consegue che, con l'incremento delle potenzialità di internet, la criminalità informatica ha costituito una rete volta a scambiare informazioni e commercializzare prodotti e servizi funzionali al compimento di reati[6]. La possibilità di ricorrere a un mercato internazionale che possa gestire un sistema informatico vasto, ha esteso lo scenario del cyber-crime a qualsiasi tipologia di organizzazione criminale o terroristica.

5 Cfr. RESEARCH CENTER OF CYBER INTELLIGENCE AND INFORMATION SECURITY - SAPIENZA UNIVERSITÀ DI ROMA, (a cura di R. BALDONI e L. MONTANARI), 2015 Italian Cyber Security Report, Un Framework Nazionale per la Cyber Security, in http://www.cybersecurityframework.it.
6 Cfr. AGENZIA PER L'ITALIA DIGITALE, (a cura di A. RAGOSA), La strategia e le azioni AgID per la gestione della sicurezza informatica delle P.A., in http://www.agid.gov.it.

In tale contesto, sono state rilevate ampie lacune nei sistemi utilizzati dalle P.A.[7], che hanno reso opportuna la costituzione di autorità ed enti ad hoc. È sorta, quindi, la necessità di incrementare e migliorare la protezione informatica delle P.A., con l'obiettivo di ridurre la vulnerabilità dei sistemi, nonché di diffondere la conoscenza delle norme a tutela della cyber security. Inoltre, sono stati definiti in maniera più attenta gli scenari di valutazione del rischio, coinvolgendo strutture adeguate e creandole laddove non esistenti, e costruendo una vera e propria cultura di monitoraggio e aggiornamento costante delle procedure, delle prassi e degli strumenti utilizzati.

È sufficiente verificare i rapporti tecnici di pochi anni fa per notare che la situazione della pubblica amministrazione è evoluta e si sta adeguando agli obiettivi europei. A titolo esemplificativo, il rapporto annuale del CIS (Centro di Ricerca Cyber Security della Università La Sapienza di Roma) fornisce un'idea chiara delle mancanze delle amministrazioni, anche delle più importanti e complesse[8].

2. AGID e CONSIP: due facce della stessa medaglia. Per comprendere la complessa architettura istituzionale che è stata creata dal legislatore nazionale, occorre definire due degli attori principali che operano all'interno di questa struttura: AgID e Consip.

L'Agenzia per l'Italia Digitale o AgID è stata istituita nel 2012 (art. 19 del Decreto Sviluppo) ed è sottoposta alla vigilanza del Presidente del Consiglio dei ministri o di un ministro delegato. Si tratta di un ente pubblico non economico avente il compito di fornire alle amministrazioni il supporto conoscitivo essenziale per l'attività amministrativa, che opera sulla base dei principi di autonomia organizzativa, tecnico-operativa, gestionale, di trasparenza e di

7 Le pubbliche amministrazioni, anche ai sensi della legge sul procedimento amministrativo (l. 7 agosto 1990, n. 241, art. 3-bis), incentivano l'uso della telematica nei rapporti interni tra le diverse amministrazioni e tra queste e i privati, al fine di conseguire una maggiore efficienza nella loro attività.

8 Cfr. RESEARCH CENTER OF CYBER INTELLIGENCE AND INFORMATION SECURITY - SAPIENZA UNIVERSITÀ DI ROMA, 2014 Italian Cyber Security Report, Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione Italiana, in http://www.agid.gov.it.

economicità e «persegue gli obiettivi di efficacia, efficienza, imparzialità, semplificazione e partecipazione dei cittadini e delle imprese».

Come espressamente stabilito dall'art. 14-bis del Codice dell'amministrazione digitale[9], la sua funzione principale è quella di essere preposta alla realizzazione degli obiettivi dell'Agenda digitale italiana e dell'Agenda digitale europea, promuovere l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della P.A. e nel rapporto tra questa, i cittadini e le imprese[10].

9 Norma inserita dal d.lgs. 26 agosto 2016, n. 179.

10 Ai sensi dell'art. 14-bis, comma 2, del Codice dell'amministrazione digitale, le specifiche funzioni dell'AgID sono le seguenti: «a) emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea; b) programmazione e coordinamento delle attività delle amministrazioni per l'uso delle tecnologie dell'informazione e della comunicazione, mediante la redazione e la successiva verifica dell'attuazione del Piano triennale per l'informatica nella pubblica amministrazione contenente la fissazione degli obiettivi e l'individuazione dei principali interventi di sviluppo e gestione dei sistemi informativi delle amministrazioni pubbliche. Il predetto Piano è elaborato dall'AgID, anche sulla base dei dati e delle informazioni acquisiti dalle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo n. 165 del 2001, ed è approvato dal Presidente del Consiglio dei ministri o dal Ministro delegato entro il 30 settembre di ogni anno; c) monitoraggio delle attività svolte dalle amministrazioni in relazione alla loro coerenza con il Piano triennale di cui alla lettera b) e verifica dei risultati conseguiti dalle singole amministrazioni con particolare riferimento ai costi e benefici dei sistemi informatici secondo le modalità fissate dalla stessa Agenzia; d) predisposizione, realizzazione e gestione di interventi e progetti di innovazione, anche realizzando e gestendo direttamente o avvalendosi di soggetti terzi, specifici progetti in tema di innovazione ad essa assegnati nonché svolgendo attività di progettazione e coordinamento delle iniziative strategiche e di preminente interesse nazionale, anche a carattere intersettoriale; e) promozione della cultura digitale e della ricerca anche tramite comunità digitali regionali; f) rilascio di pareri tecnici, obbligatori e non vincolanti, sugli schemi di contratti e accordi quadro da parte delle pubbliche amministrazioni centrali concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati per quanto riguarda la congruità tecnico-economica, qualora il valore lordo di detti contratti sia superiore a euro 1.000.000,00 nel caso di procedura negoziata e a euro 2.000.000,00 nel caso di procedura ristretta o di procedura aperta. […]; g) rilascio di pareri tecnici, obbligatori e non vincolanti, sugli elementi essenziali delle procedure di gara bandite, ai sensi dell'articolo 1, comma 512 della legge 28 dicembre 2015, n. 208, da Consip e dai soggetti aggregatori di cui all'articolo 9 del decreto-legge 24 aprile 2014, n. 66, concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati e definiti di carattere strategico nel piano triennale. Ai fini della presente lettera per elementi essenziali si intendono l'oggetto della fornitura o del servizio, il valore economico del contratto, la tipologia di procedura che si intende adottare, il criterio di aggiudicazione e relativa ponderazione, le principali clausole che caratterizzano le prestazioni contrattuali. Si applica quanto previsto nei periodi da 2 a 5 della lettera f); h) definizione di criteri e modalità per il monitoraggio sull'esecuzione dei contratti da parte dell'amministrazione interessata ovvero, su sua richiesta, da parte della stessa AgID; i) vigilanza sui servizi fiduciari ai sensi dell'articolo 17 del regolamento UE 910/2014 in qualità di organismo a tal fine

Per quanto concerne Consip S.p.A., si tratta di un modello societario particolare e innovativo. Essa è stata la prima centrale di committenza pubblica in Italia specializzata nella gestione di tutte le fasi del processo di approvvigionamento, con le funzioni di pianificazione strategica degli acquisti e di supporto nella gestione del procedimento di acquisizione. Consip ha svolto tali funzioni attraverso l'ausilio delle moderne tecnologie informatiche ed è stata in grado di rendere trasparente e celere il complesso meccanismo burocratico concernente l'approvvigionamento di beni e servizi pubblici (GIARDETTI, 2015)
Consip, costituita prima dell'AgID (nell' agosto 1997), è divenuta uno strumento di cambiamento della gestione delle tecnologie dell'informazione nell'allora Ministero del Tesoro, del Bilancio e della Programmazione Economica. Successivamente, mediante d.m. del 24 febbraio 2000 è stato conferito a Consip l'incarico di stipulare convenzioni e contratti quadro per l'acquisto di beni e servizi per conto delle Pubbliche Amministrazioni. Consip è stata, pertanto, garante dell'effettivo ed efficiente impiego delle tecnologie informatiche nel settore pubblico.

A partire dal 2012[11] le funzioni di supporto alle amministrazioni pubbliche in materia informatica sono state trasferite da Consip a Sogei S.p.A.[12], attraverso l'attribuzione delle attività informatiche riservate allo Stato e dello sviluppo e della gestione dei sistemi informatici destinati al settore pubblico. Consip continua, invece, a gestire l'attività di acquisizione dei beni e servizi per

designato, sui gestori di posta elettronica certificata, sui soggetti di cui all'articolo 44-bis, nonché sui soggetti, pubblici e privati, che partecipano a SPID di cui all'articolo 64; nell'esercizio di tale funzione l'Agenzia può irrogare per le violazioni accertate a carico dei soggetti vigilati le sanzioni amministrative di cui all'articolo 32-bis in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza; l) ogni altra funzione attribuitale da specifiche disposizioni di legge e dallo Statuto».

11 D.l. 27 giugno 2012 , n. 87, concernente misure urgenti in materia di efficientamento, valorizzazione e dismissione del patrimonio pubblico, di razionalizzazione dell'amministrazione economico-finanziaria, nonché misure di rafforzamento del patrimonio delle imprese del settore bancario.

12 Sogei (Società Generale d'Informatica S.p.A.) è la società di Information Technology totalmente controllata dal Ministero dell'Economia e delle Finanze e opera sulla base del modello organizzativo dell'in house providing. È partner tecnologico unico del citato Ministero, ha progettato e realizzato il Sistema informativo della fiscalità, del quale segue conduzione ed evoluzione e sviluppa sistemi, applicazioni e servizi per le esigenze di automazione e informatizzazione dei processi operativi e gestionali del Ministero, della Corte dei conti, delle Agenzie fiscali e di altre pubbliche amministrazioni.

Sogei e opera anche al servizio dell'AgID, svolgendo funzioni relative alle Reti telematiche della pubblica amministrazione, al Sistema pubblico di Connettività o SPC, alla Rete internazionale della P.A. e ai contratti quadro finalizzati alla rimozione delle duplicazioni amministrative di carattere informatico[13].

Dall'altro lato della medaglia, l'AgID interagisce con Consip mediante il rilascio di pareri tecnici, obbligatori e non vincolanti, sugli elementi essenziali delle procedure di gara bandite da Consip concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati e di carattere strategico nel piano triennale[14].

La funzione che aveva originariamente Consip, quale affidataria delle procedure informatiche riservate allo Stato è stata fortemente riformulata e considerata funzionale esclusivamente per l'espletamento delle attività collegate al proprio ruolo di centrale di committenza nazionale per l'acquisto di beni e servizi per il settore amministrativo pubblico[15].

Con particolare riferimento alla sicurezza cibernetica, a Consip, in collaborazione con l'AgID, viene affidato il compito di gestire e indirizzare le richieste del settore pubblico al fine di rendere il sistema informatico della P.A. più efficiente e sicuro.

Vediamo ora come si intersecano i ruoli dei due attori AgID e Consip con le recenti direttive normative in tema di cyber security.

13 Ai sensi dell'art. 4, comma 3-ter, del d.l. 6 luglio 2012, n. 95, convertito dalla l. 7 agosto 2012, n. 135, è stabilito che «Fermo restando lo svolgimento da parte di Consip S.p.A. delle attività ad essa affidate con provvedimenti normativi, le attività di realizzazione del Programma di razionalizzazione degli acquisti, di centrale di committenza e di e-procurement continuano ad essere svolte dalla Consip S.p.A. Ferme restando le disposizioni di cui all'articolo 12, commi da 2 a 10, del decreto-legge 6 luglio 2011, n. 98, convertito, con modificazioni, dalla legge 15 luglio 2011, n. 111, gli strumenti di acquisto e di negoziazione messi a disposizione da Consip S.p.A. possono avere ad oggetto anche attività di manutenzione. La medesima società svolge, inoltre, le attività ad essa affidate con provvedimenti amministrativi del Ministero dell'economia e delle finanze. Sogei S.p.A., sulla base di apposita convenzione disciplinante i relativi rapporti nonché i tempi e le modalità di realizzazione delle attività, si avvale di Consip S.p.A, nella sua qualità di centrale di committenza, per le acquisizioni di beni e servizi».

14 Cfr. supra art. 14-bis, comma 2, del Codice dell'amministrazione digitale.

15 Cfr. M. DE BENEDETTI, Public procurement e cyber sicurezza nella P.A., in www.sicurezzanazionale.gov.it.

3. Verso un'architettura istituzionale di sicurezza cibernetica. Come anticipato, ogni amministrazione presenta caratteristiche differenti, per dimensioni, complessità organizzativa, tipologia di dati trattati. Il livello di esposizione ai rischi cibernetici aumenta e dipende anche da fattori ambientali e politici e ciò ha portato a prevedere una differenziazione nella disciplina della sicurezza, istituendo un'architettura distinta su tre livelli di intervento che vedremo più avanti nel dettaglio.

Con la legge di stabilità del 2016[16] il legislatore ha inteso porsi quale obiettivo principale il risparmio di spesa annuale della pubblica amministrazione per la gestione del settore informatico, mediante le seguenti modalità: (i) redazione di un Piano Triennale per l'informatica nella pubblica amministrazione da parte dell'AgID, contenente, per ciascuna amministrazione o categoria di amministrazioni, l'elenco dei beni e servizi informatici e di connettività e dei relativi costi, suddivisi in spese da sostenere per innovazione e spese per la gestione corrente, individuando altresì i beni e servizi la cui acquisizione riveste particolare rilevanza strategica; (ii) programmazione di acquisti di beni e servizi per l'informatica da parte di Consip o del soggetto aggregatore interessato e previa consultazione con l'AgID in merito ai beni e servizi strategici individuati nel citato Piano triennale; e (iii) risparmio di spesa annuale, da raggiungere alla fine del triennio 2016-2018, pari al 50 per cento della spesa annuale media per la gestione corrente sostenuta da ciascuna amministrazione per il solo settore informatico nel triennio 2013-2015.

Nelle more della definizione del Piano triennale, con circolare del 24 giugno 2016[17], l'AgID ha fornito le modalità con cui le amministrazioni pubbliche e le società inserite nel conto economico consolidato della P.A. individuate dall'ISTAT possono procedere agli acquisti di beni e servizi ICT (Information Communication Technology).

16 Art. 1, commi da 512 a 516, della l. 28 dicembre 2015, n. 208, Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato.
17 Circolare AgID n. 2 del 24 giugno 2016, «Modalità di acquisizione di beni e servizi ICT nelle more della definizione del "Piano triennale per l'informatica nella pubblica amministrazione" previsto dalle disposizioni di cui all'art.1, comma 513 e seguenti della legge 28 dicembre 2015, n.208 (Legge di stabilità 2016)».

La circolare in questione si inserisce nel più ampio contesto dei poteri conferiti all'AgID dal nuovo Codice dei Contratti Pubblici (d.lgs. 18 aprile 2016, n. 50) che, all'art. 58, comma 10, stabilisce che l'AgID «deve emanare le regole tecniche aggiuntive per garantire il colloquio e la condivisione dei dati tra i sistemi telematici di acquisto e negoziazione». Regole tecniche che sono state definite con la successiva circolare del 6 dicembre 2016[18] e che individuano le modalità con cui possono interoperare le piattaforme telematiche di e-procurement, stabilendo i riferimenti per l'utilizzo condiviso dei dati scambiati tra le piattaforme. L'obiettivo perseguito è quello di contribuire alla trasparenza delle fasi del processo e alla maggiore competitività tra fornitori di beni e servizi, nonché alla salvaguardia della spesa pubblica.

Contestualmente il legislatore europeo ha emanato una direttiva di notevole impatto sul tema oggetto di esame: la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza informatica nazionali (la c.d. Direttiva NIS). Si tratta di una normativa estesa a tutti gli Stati membri dell'Unione, che dovrà essere recepita entro maggio 2018. In Italia non è stata ancora emanata la relativa legge di attuazione, la quale indicherà nel dettaglio le specifiche azioni da intraprendere. Tra le disposizioni di maggiore rilevanza, la Direttiva NIS prevede (i) il miglioramento della capacità di cyber security dei singoli Stati dell'Unione mediante l'adozione di specifiche misure di sicurezza a carico dei settori interessati, (ii) l'aumento del livello di cooperazione tra gli Stati membri, (iii) l'obbligo per gli operatori di servizi essenziali e dei fornitori di servizi digitali di adottare un approccio basato sulla gestione dei rischi, nonché di riportare ad un'apposita autorità (e in ultima analisi all'Agenzia europea ENISA) tutti gli incidenti di una certa entità, e (iv) la designazione da parte di ogni Stato membro di un'autorità apposita che sia il punto di contatto per gli scambi

18 Circolare AgID n. 3 del 6 dicembre 2016, «Regole Tecniche aggiuntive per garantire il colloquio e la condivisione dei dati tra sistemi telematici di acquisto e di negoziazione».

internazionali, nonché la dotazione di una strategia cyber e la costituzione di uno o più CERT e CSIRT[19].

Occorre notare che l'Italia, in linea con le linee tracciate dalla Direttiva NIS, si è portata avanti emanando il 17 febbraio 2017 un decreto contenente gli indirizzi per la protezione cibernetica e la sicurezza informatica nazionali[20]. Il decreto ha permesso la riorganizzazione dell'architettura istituzionale della cyber security nazionale[21], già disciplinata peraltro nel previgente e analogo decreto del 24 gennaio 2013[22], rendendola più snella ed efficace. Tra le linee di intervento più innovative, si ravvisa il rafforzamento del ruolo del CISR (Comitato interministeriale per la sicurezza della Repubblica), che potrà emanare direttive con l'obiettivo di incrementare il livello di sicurezza informatica sul territorio nazionale e si avvarrà del supporto del CISR tecnico, ossia del coordinamento interministeriale delle amministrazioni CISR e del Dipartimento delle informazioni per la sicurezza (DIS). Inoltre, il nuovo decreto attribuisce al Direttore generale del DIS il compito di definire le linee di azione per la sicurezza cibernetica che dovranno assicurare i necessari livelli di sicurezza dei sistemi e delle reti di interesse strategico, sia pubblici che privati,

19 Per completezza, si segnala che l'acronimo inglese CERT sta per Computer Emergency Response Team, ossia squadra per la risposta ad emergenze informatiche, mentre CSIRT (Computer Security Incident Response Team) è la squadra preposta a rispondere in caso di incidenti informatici.

20 D.p.c.m. 17 febbraio 2017, n. 110835 «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali», pubblicato in Gazzetta Ufficiale n. 87 del 13 aprile 2017.

21 L'art. 1 del d.p.c.m. del 17 febbraio 2017 citato supra, fa riferimento alla «architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali».

22 D.p.c.m. 24 gennaio 2013, n. 67251 «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali», abrogato dall'art. 13, comma 4, del d.p.c.m. 17 febbraio 2017 citato supra. Rispetto a tale decreto, con il d.p.c.m. del 17 febbraio 2017 viene ampliata la definizione di sicurezza cibernetica, aggiungendo il termine controllo indebito. Ora la sicurezza cibernetica è definita pertanto quale: «condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria o accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel controllo indebito, danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi». Stessa estensione è stata data dal legislatore anche alle definizioni di minaccia cibernetica ed evento cibernetico (art. 2 del d.p.c.m. del 17 febbraio 2017).

verificandone ed eliminandone le vulnerabilità[23]. Ancora, con il decreto del 17 maggio 2017, il Nucleo sicurezza cibernetica o NSC viene ricondotto all'interno del DIS con l'obiettivo di fornire risposte agli eventi cibernetici significativi in raccordo con le strutture dei ministeri competenti per materia. Con particolare riferimento all'AgID, è prevista una forte interazione dell'agenzia con il Dipartimento della funzione pubblica e con alcuni ministeri (MiSE, Ministero dell'interno, Ministero della difesa e MEF). La ratio di tale intervento normativo è stata quella di raggiungere una maggiore semplificazione e razionalizzazione dell'impianto di cyber security, migliorando anche le funzioni di coordinamento e raccordo delle attività di prevenzione, preparazione e gestione delle crisi cibernetiche.

Con il decreto del 17 febbraio 2017 permangono in capo al Presidente del Consiglio dei ministri i poteri previsti in precedenza quale, a titolo esemplificativo, quello di adottare, su deliberazione del CISR, il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali[24], e le linee d'azione da porre in essere per realizzare il quadro strategico nazionale[25].

A valle del decreto sinora esaminato, l'AgID, in attuazione del d.l. 22 giugno 2012, n. 83[26] e della direttiva del Presidente del Consiglio dei ministri del 1° agosto 2015, che ha imposto l'adozione di standard minimi di prevenzione e reazione agli eventi cibernetici[27], ha emanato le Misure minime di sicurezza ICT

23 Art. 6 del d.p.c.m. 17 febbraio 2017 citato supra.
24 L'ultimo Piano nazionale è stato adottato il 31 marzo 2017: stabilisce gli obiettivi da perseguire e individua la roadmap per l'adozione da parte di soggetti pubblici e privati delle misure prioritarie per l'implementazione del quadro strategico nazionale (cfr. infra), sulla base di un dialogo attivo e interattivo (in particolare, prevede ben undici indirizzi operativi, tra i quali, ad esempio, la promozione e diffusione della cultura della sicurezza informatica, l'implementazione di un sistema di cyber risk management nazionale).
25 Quadro Strategico Nazionale adottato dalla Presidenza del Consiglio dei ministri nel dicembre 2013. Cfr. anche l'art. 3 del d.p.c.m. 17 febbraio 2017 citato supra.
26 L'art. 20, comma 3, lett. b) del d.l. 22 giugno 2012, n. 83, identifica nell'AgID l'organismo che «detta indirizzi, regole tecniche e linee guida in materia di sicurezza informatica».
27 La direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri ha individuato l'AgID quale organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento in linea con quelli dei maggiori Stati partners e delle organizzazioni internazionali di cui l'Italia è parte. Si legge nella direttiva: «è emersa innanzitutto l'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di

per le Pubbliche Amministrazioni. Tali misure sono contenute nella circolare AgID n. 1 del 17 marzo 2017 e sono entrate in vigore con la pubblicazione in Gazzetta Ufficiale il 4 aprile 2017. Tuttavia le misure sono state rese pubbliche dall'AgID già un anno prima (i.e. il 26 aprile 2016): si è trattato di un'anticipazione della regolamentazione che è stata ufficializzata in seguito e che ha fornito alle P.A. dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento. La strategia adottata dall'AgID è stata certamente utile per le amministrazioni, specie in ragione della scadenza del 31 dicembre 2017, entro la quale dovranno essere attuati gli adempimenti previsti dalla circolare.

Con riferimento al contenuto delle misure anzidette, si rileva che l'AgID prevede tre livelli di attuazione: un livello minimo contenente i criteri di base cui la P.A. indipendentemente dalla sua dimensione o natura dovrà conformarsi in termini tecnologici, organizzativi e procedurali; altri due livelli che rappresentano standard di protezione più completi ed evoluti, che dovrebbero essere adottati dalle organizzazioni maggiormente esposte a rischi, specialmente se trattano informazioni o prestano servizi di particolare complessità e criticità.

L'AgID, con le misure in esame, intende fornire delle linee guida operative per proteggere i sistemi informativi e i dati delle pubbliche amministrazioni, permettendo una autovalutazione delle esigenze operative e delle mancanze della struttura ICT e l'individuazione delle azioni da intraprendere per il relativo adeguamento.

Per la tutela del proprio patrimonio informatico, le pubbliche amministrazioni hanno la possibilità di accedere a servizi in grado di mantenere il personale aggiornato sui rischi e sulle lacune della sicurezza cibernetica. Le P.A. dovrebbero, perciò, essere in grado di valutare e correggere le problematiche riscontrate e attuare policies idonee alla tipologia di struttura che è propria di un ente pubblico.

---

eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi».

Ultimo tassello del mosaico sopra rappresentato è la recente adozione del Piano Triennale per l'informatica nella pubblica amministrazione 2017-2019, predisposto dall'AgID (in collaborazione con, tra gli altri, Consip) e firmato dal Presidente del Consiglio dei ministri il 31 maggio 2017. È un documento di programmazione che definisce il percorso di attuazione nel modello strategico di evoluzione del sistema informativo della P.A., preventivando le spese per singola amministrazione o categoria di amministrazione in coerenza con gli obiettivi da raggiungere. Con questo documento l'AgID intende guidare da un punto di vista operativo la trasformazione digitale delle pubbliche amministrazioni, definendo le linee guida della strategia di sviluppo dell'informatica pubblica e fissando i principi e le regole per perseguire tale sviluppo.

Come rilevato anche dalla stessa AgID, il Piano Triennale non funge da libretto di istruzioni definitivo e completo; risulterebbe, infatti, difficile pianificare gli investimenti caso per caso. Pertanto è stato ideato un processo che sia di supporto all'interpretazione del Piano stesso e che integri in una fase successiva il documento. Al riguardo, si segnala che il Piano Triennale pubblicato il 31 maggio 2017 definisce le azioni per l'anno 2018, tuttavia, a settembre 2018 (e a settembre di ogni anno) verrà pubblicata una versione aggiornata del testo contenente le azioni previste per l'anno successivo, su proposta dell'AgID e previa approvazione del Presidente del Consiglio dei ministri o del Ministro delegato. In altre parole, si tratta di un piano in continua evoluzione.

Il lavoro svolto dall'AgID prosegue non solo nell'aggiornamento e integrazione del Piano Triennale ma anche nella predisposizione di una serie di linee guida contenente le specifiche tecnologiche e le scelte di indirizzo. A titolo esemplificativo, entro il mese di gennaio 2018 è previsto il rilascio di Linee guida per la razionalizzazione del patrimonio ICT delle P.A..

Il Piano Triennale prevede, inoltre, una specifica sezione dedicata alla sicurezza, rilevandone l'importanza per garantire la disponibilità, l'integrità e la riservatezza delle informazioni proprie del sistema informativo della P.A.[28]
L'AgID si occuperà del monitoraggio e del controllo dell'applicazione del Piano Triennale da parte delle amministrazioni, all'interno delle quali dovrà essere individuato un Responsabile della Trasformazione Digitale, preposto al confronto e al dialogo con l'AgID. Al riguardo, si è posta la domanda sulle possibili conseguenze in caso di ritardo nell'adeguamento da parte di un'amministrazione alle azioni descritte nel Piano Triennale. L'AgID ha fornito in merito una risposta piuttosto generica, senza individuare le relative sanzioni: «Ogni ritardo […] è da considerarsi come un costo non necessario per lo Stato, che deve essere ostacolato con i necessari strumenti di controllo della spesa pubblica».

4. Possibili criticità e considerazioni conclusive. Se per decenni la questione della sicurezza informatica era celata ed accessibile solo agli addetti ai lavori, oggi si discute apertamente e in maniera approfondita sulle minacce cibernetiche e su argomenti che erano ritenuti troppo tecnici.
Ne deriva una forte convinzione che sia necessario dotarsi di norme e strutture condivise che coordinino la materia complessiva della cyber security per i sistemi nazionali e sovranazionali in un'ottica di collaborazione: tutti devono partecipare e coadiuvare le proprie risorse, informazioni, capacità ed esperienze.

Non possono, tuttavia, nascondersi le criticità che derivano dalla implementazione dell'architettura di sicurezza cibernetica qui esaminata, specie con riferimento all'attuazione delle misure minime di sicurezza da parte della P.A. di cui alla circolare AgID n. 1 del 17 marzo 2017 sopra citata.

28 Sono previsti obiettivi strategici e linee di azione tra cui risulta, a titolo esemplficativo, (i) la realizzazione e gestione di un catalogo delle vulnerabilità informatiche (National Vulnerability Database - NVD), che va ad integrare i cataloghi disponibili a livello internazionale, con le vulnerabilità riscontrate in ambito nazionale, (ii) la realizzazione della Cyber Security Knowledge Base nella quale sono raccolte le informazioni sulle infrastrutture realizzate nel dominio della P.A. e sugli eventi di sicurezza occorsi nel tempo al loro interno.

La principale problematica è la mancanza di risorse della P.A.. Occorrono adeguate dotazioni finanziarie e l'adozione di tali misure è eccessivamente onerosa, specie se si tratta di implementare il terzo livello di applicazione, che consiste in un livello costoso, suggerito per le amministrazioni più grandi e più complesse, che erogano servizi aventi un maggiore livello di criticità. Dovranno essere fatti inevitabilmente degli investimenti.

Inoltre, non è da sottovalutare, la formazione adeguata del personale dipendente delle Pubbliche Amministrazioni, che si troveranno di fronte a novità di rilievo, con un notevole impatto sull'attività lavorativa dagli stessi svolta. Occorrerà sensibilizzare i dipendenti pubblici affinché siano evitati errori e siano diminuiti i rischi di condotte incaute o erronee di soggetti che non hanno dimestichezza con tale settore.

Riferimenti bibliografici

AGENZIA PER L'ITALIA DIGITALE (a cura di A. RAGOSA), La strategia e le azioni AgID per la gestione della sicurezza informatica delle P.A., in http://www.agid.gov.it.

E. CASETTA- F. FRACCHIA, Compendio di diritto amministrativo, Giuffrè Editore, Milano, 2016.

M. DE BENEDETTI, Public procurement e cyber sicurezza nella P.A., in www.sicurezzanazionale.gov.it

A. GIARDETTI, Il modello Consip evoluzione e funzioni della centrale di committenza nazionale, Key Editore, Vicalvi, 2015.

RESEARCH CENTER OF CYBER INTELLIGENCE AND INFORMATION SECURITY - SAPIENZA UNIVERSITÀ DI ROMA, (a cura di R. BALDONI e L. MONTANARI), 2015 Italian Cyber Security Report, Un Framework Nazionale per la Cyber Security, in *http://www.cybersecurityframework.it*.

RESEARCH CENTER OF CYBER INTELLIGENCE AND INFORMATION SECURITY - SAPIENZA UNIVERSITÀ DI ROMA, 2014 Italian Cyber Security Report, Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione Italiana, in http://www.agid.gov.it.

Agency Reform in the time of Cybersecurity Governance: ENISA

by **ELENA PAURI**

Abstract

L'Agenzia Europea per la sicurezza delle reti e dell'informazione (ENISA) ha recentemente ricevuto dal Mediatore Europeo il premio per la Buona Amministrazione "Eccellenza nell'Innovazione", in virtù del suo progetto dedicato alla ridefinizione della cooperazione europea nel settore della sicurezza informatica.
Tuttavia, nonostante i notevoli risultati raggiunti in termini di qualità dell'output, in appena tredici anni di vigenza ENISA è stata soggetta a molteplici riforme che hanno modificato il suo regolamento istitutivo. Inoltre, ENISA è oggi soggetta ad un ulteriore processo di riforma. Alla luce dei risultati ottenuti dalla consultazione pubblica lanciata dalla Commissione Europea nel 2017, il presente articolo si occuperà dell'impatto che il sempre crescente rischio informatico ha sul cosiddetto "modello di agenzia europea". A tal fine sarà fornita, in primo luogo, una panoramica generale della normativa che regola ENISA. In secondo luogo, verranno analizzate le precedenti modifiche normative e le recenti proposte di riforma relative all'Agenzia, anche alla luce della dottrina tradizionale di settore. In seguito ci si interrogherà sulla capacità dell'Agenzia di rispettare i più elevati standard di diritto amministrativo rispetto alla "Dichiarazione congiunta e all'approccio comune" (*Joint Statement and Common Approach)* concordato nel luglio 2012 dal Gruppo di lavoro interistituzionale sulle agenzie decentralizzate dell'Unione europea. In conclusione verrà sostenuto che, come dimostrato dall'odierna minaccia nel settore della sicurezza informatica, vi è la necessità che le riforme delle agenzie europee assumano carattere meno frammentario e vadano oltre lo *status quo* attuale nella governance europea.

1. Introduction. In may 2017, a ransomware cyber-attack compromised hospitals' security in England and spread to more than 150 countries across the world. According to the European Cybercrime Centre (EC3), an observatory body set up in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus help protect European citizens, businesses and governments from

online crime, the financial cost of cybercrime for EU Member States (hereafter, MSs) is around €265 billion per year (EUROPOL 2017).

According to the European Commission, «[c]yber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein» (JOIN(2013)1 FINAL). The Commission has highlighted that cybersecurity is a high concern for many EU citizens in order to engage in e-commerce and for around a third of small to medium Enterprises to offer online services (COM/2010/245 F/2). According to a recent survey, at least 80% of European companies have experienced at least one cybersecurity incident over the 2014 (PWC.org 2017). If citizens and business owners lack confidence in security, it stands to reason that they may avoid participating in online activities, thereby inhibiting further development opportunities on cyberspace (ENISA 2014).

Notwithstanding existing threats, the benefits of cyber-reality are far superior to its disadvantages. Cyberspace offers an outstanding opportunity for social and economic growth, urging MSs and international organisations to tackle the issue of cybersecurity on the basis of mutual cooperation and information sharing. In fact, «national governments are best placed to organise the prevention and response to cyber incidents» (JOIN(2013)1 FINAL) and ENISA is called to be their expertise-based point of reference[1].

2. The European Union Agency for Network and Information Security (ENISA) and EU cyber governance. ENISA (hereafter, also “the Agency”) was set up in 2004 as a decentralised agency with the overall goal of ensuring a high level of network and information security (NIS) within the EU, thus contributing to the smooth functioning of the internal market (REGULATION (EC) NO 460/2004;

1 However, different policy approaches to coordination exist and they not always align. See, for instance, A. BOIN - M . BUSUIOC - M. GROENLEER, 2014.

MCKENNA 2004). ENISA has since supported European institutions, MSs and the business community in addressing, responding to and preventing NIS problems by developing and maintaining a high level of expertise in cybersecurity; supporting institutional cooperation and the implementation of EU policy; strengthening the MSs, EU institutions, agencies and bodies' capability and preparedness to prevent, detect and respond to NIS problems and incidents; identifying emerging trends and needs in view of evolving cybercrime and cybersecurity patterns. The Regulation also provides a definition of NIS as «the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and related services offered by or accessible via these networks and systems» (REGULATION (EC) NO 4 I60/2004).

The Agency was deemed to operate as a point of reference «establishing confidence by virtue of its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in performing the tasks assigned to it» (*ibid*.). Thus, ENISA was provided with expertise-based advisory powers and the capacity to facilitate and promote cooperation among EU institutions, MSs as well as third countries (*ibid*.). The Agency has its seat in Heraklion and a secondary branch in Athens, Greece.

In line with the common EU agency structure and according to the latest amendments, the bodies of ENISA comprise a Management Board (composed by representatives from MSs and the Commission) which defines the general orientations for the operation of the Agency, an Executive Director appointed by the Management Board and responsible of the day-to-day administration of the Agency, and a Permanent Stakeholders Group (composed by experts from the ICT industry, e-communication providers, consumers, academia and representatives from MSs' regulatory authorities) chaired by the Director to perform advisory duties. ENISA's annual and multiannual working programmes as well as the final annual report are approved by the Management Board on

proposal by the Executive Director. The programme is then forwarded to the European Parliament, the Council, the Commission and the Member States and published. However, the Commission is the institution under which ENISA performs its mission. In fact, the Commission is involved in the appointment of the Agencies members, the proposal of the working programme and the drafting of the annual budget.

Since ENISA was first set up, it has been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships (CENCETTI 2014; MCKENNA 2013).

Thanks to its project on Redefining European cyber cooperation[2], ENISA recently received the EU Ombudsman Award for Good Administration for Excellence in Innovation.

3. An evolving frame work: setting and early reforms. Notwithstanding its incredible results in terms of output quality, in barely 13-years lifetime ENISA has gone through several reforms.

In 2008, an amendment to the Regulation establishing ENISA extended the mandate of the Agency for a period of 3 years. In fact, ENISA was first established for a period of 5 years so that its mandate was supposedly due to expire in 2009 (REGULATION (EC) NO 107/2008).

Following further debate, in 2009 the Council took the view that «[a]n enhanced and holistic European strategy for NIS, with clearly delineated roles of the European Commission, the Member States and ENISA, is of vital importance to tackle current and future challenges» (COUNCIL RESOLUTION 2009). However, notwithstanding the need to proceed with a thorough reform of the Agency mandate and powers, instead of amending Regulation (EC) No 460/2004, the duration of the Agency was once again extended until 13 September 2013 (REGULATION (EU) NO 580/2011).

2 A cyber-crisis simulation executed in real-time (over 48 hours) following two years of planning thanks to which training was provided to more than 1000 participants. See more at https://www.enisa.europa.eu/news/enisa-news/enisa-wins-award-for-excellence-in-innovation-transformation-at-eu-ombudsman-award-for-good-administration

With the Cybersecurity Strategy of the European Union (JOIN(2013)1 FINAL), the Commission gave new stimulus to the EU cybersecurity's policy. Even though the Strategy did not mean to amend ENISA's mandate, the Commission urged ENISA to perform particular tasks including the evaluation of the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs)[3] for the EU, the provision of technical guidelines and recommendations for the adoption of NIS good practices and the proposal of a roadmap for a "Network and Information Security driving licence" as a voluntary certification programme to promote enhanced skills of IT professionals (*ibid*.).

In 2013, a new Regulation (NO 526/2013) was provided to modernise and extend ENISA's mandate, also in view of the increasement of its links with Europol and industry stakeholders (COM(2013) 48 FINAL). Firstly, the Agency was given an increased budgetary allowance in order to support its contribute not only to the implementation of a high level of NIS but also to ensure better protection of privacy and personal data and the proper functioning of the internal market (REGULATION NO 526/2013). Secondly, the Agency was given new tasks, including the establishment and operation of a peer-review system to develop the CERTs capabilities (*ibid*.). Thirdly, the Agency was reformed in view of the need for it to be compliant with the principles of subsidiarity, independence, transparency and those laid down in the Joint Statement and Common Approach agreed upon in July 2012 by the Inter-Institutional Working Group on EU decentralised agencies (*ibid*.). ENISA was also given new objectives, e.g. assisting the Union institutions, bodies, offices, agencies and MSs to meet the legal and regulatory requirements of NIS under existing and future legal acts of the Union (art 3.3) and tasks, e.g. disseminating data (art. 4(1)(b)(vi)) and facilitating the technical standardisation process (art. 4(1)(d)(i)). However, the

3 A Computer Security Incident Response Teams (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. A Computer Emergency Response Team (CERT) is developed in both private and public sectors in small teams of cyber-experts connected to the internet that can effectively and efficiently respond to information security incidents and cyber threats, often on a 24 hours a day-7days a week basis. See more about CERT-EU at https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html.

main change is perhaps to be acknowledged in the different approach the EU legislator adopts with regards to the best suited policy level to face modern cybersecurity threats. In fact, instead of maintaining its traditional understanding i.e. that MSs are best placed to engage in cybersecurity active policy, the EU now envisages to adopt new measures in accordance with the principles of subsidiarity and proportionality that «cannot be sufficiently achieved» by the Member States (*ibid.*).

The latest reform was long envisaged because of the evolving nature of the cybersecurity landscape. As mentioned in the 2013 Regulation, «[s]ince ENISA was set up, the challenges of NIS have changed with technology, market and socio-economic developments and have been the subject of further reflection and debate. In response to the changing challenges, the Union has updated its priorities for network and information security policy» (*ibid*.).

Hence, during the last two decades, the EU has repeatedly returned on its policies in the field of information security (NIS), data protection and security in electronic communication. Recently, multiple actions have been taken in order to foster the European Digital Single Market[4] and Agenda on Security in the field of cyber-related threats (COM(2015) 185 FINAL). For instance, the Commission is now setting out a new approach on interoperability of information systems (COM(2017) 261 FINAL).

Meanwhile, ENISA, Europol/EC3 and EDA have been playing an increasingly crucial role as EU-level agencies active from the perspective of NIS, law enforcement and defence respectively (CENCETTI, 2014).

However, notwithstanding its remarkable importance in view of the growing impact of cybersecurity on the market and the need to build transnational cyber-resilience, ENISA was once more given a fixed-term mandate, due to expire in the 2020 (REGULATION NO 526/2013).

4 The Digital Single Market strategy was adopted on the 6 May 2015 and includes 16 specific initiatives which have been delivered by the Commission. The strategy is now under review (see (COM)2015/0192 final). The Commission also recently launched a public-private partnership with representatives from the industry sector that is expected to trigger EUR 1.8 billion of investment by 2020 (see 2016 Cybersecurity Communication, *infra*).

4. An evolving frame work: recent developments and the 2017 public consultation. Moreover, ENISA is nowadays under a new revision process. In fact, ENISA's mandate and objectives were to be reconciled with the renovated cybersecurity landscape, which has evolved significantly in terms of threat, technological, market and policy developments. These developments include policy and regulatory measures, in particular those set out in the 'NIS Directive' and the 2016 cybersecurity Communication, which will result in "ENISA 2.0" (COM(2016) 410 final).

A public consultation took place between 18 January and 12 April 2017. It was conducted in the context of the evaluation and review of ENISA in accordance with Article 32 of Regulation (EU) No 526/2013. Respondents[5] from 19 different MSs mostly agree that, overall, the performance of ENISA during the 2013-2016 time span was positively assessed as contributing to NIS in the EU. A majority of respondents furthermore considered ENISA to be coherently achieving either to a great or some extent its individual objectives. Moreover, ENISA's output (services, guidelines, recommendations and reports) is appreciated for its EU-level body quality.

However, respondents made it clear that, due to the evolving cybersecurity landscape and the current EU policy response, some urgent needs and gaps, including cooperation across MSs, capacity to prevent, detect and resolve large scale cyber-attacks, information sharing between different stakeholders, and protection of critical infrastructure and improved education in cybersecurity, have to be addressed. In that respect, a limited number of available instruments at EU level seem adequate but ENISA, which is regarded as the most appropriate organisation to fulfil present expectations from the general public. In order to be

5 Out of 90 responses to the consultation, more than half of the respondents answered on behalf of an organisation (industry sector enterprises and representative associations), while others responded as professionals (in cybersecurity, telecommunications and government affairs) or in their personal capacity. Contributions from the public sector were comparatively low, though respondents representing national authorities were among the highest respondent group. The highest number of responses came from residents of Germany and Belgium (15 responses each), followed by respondents from Italy (7 responses), as presented in the figure below. See also https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-european-union-agency-network-and.

fully equipped for that mission, the Agency needs to be sufficiently mandated and resourced. The Commission is now carrying out an in-depth analysis of the replies to the public consultation which will be included into the overarching ex-post evaluation of ENISA, in accordance with the evaluation criteria set out in the EU Better Regulation Guidelines (COM(2015) 215 final) assessing the effectiveness, efficiency, coherence, relevance and EU added value of the Agency. The public consultation is also meant to contribute to a reflection on policy options for, once again, the revision of ENISA's mandate.

5. Good administration and governance in the cyber area. Given the above-mentioned multiplicity of interventions which ENISA's legal framework has been and still is undergoing, one is to argue whether the Agency was properly set up in the first place. In particular, it is not clear why ENISA's mandate has to be constantly renovated.

As Chamon (2016) correctly notices, notwithstanding its "regulatory agency" status, ENISA lacks one of the main features of the kind, i.e. the permanent nature of its mandate. It is common knowledge that EU agencies are bodies set up with legal personality by virtue of an EU secondary law tool in order to perform a technical, scientific or managerial mission in a specific sector at European level, with a certain degree of structural and financial independence even though subject to EU public law (BUSUIOC - GROENLEER - TRONDAL 2010; M. CHAMON 2016; CHITI 2002; CRAIG 2012; GERADIN - MUNOZ - PETIT 2005; HARLOW - RAWLINGS, 2014; MAJONE,1997; RITTBERGER - WONKA 2011). They usually are identified with decentralised bodies both in terms of institutional functions and geographical location. While a number of different classifications about agencies in the EU legal environment do exist[6] and the so-called "European agency model" is under construction[7], yet it is very important not to confuse EU regulatory agencies and executive agencies[8].

6 The EU institutional classification of EU law agencies can be found at https://europa.eu/european-union/about-eu /agencies_en. See M. CHAMON, cit., pp. 5-15.
7 The term is shaped on the famous article by G. MAJONE (cit).
8 However, the exact meaning of that divide is still subject to much controversy. Even though the

There is no apparent reason for ENISA being established as a non-permanent body. First, even in the early 2000s it was clear to the Commission that the "way forward", as it was called in its 2008 Communication (COM(2008)135 FINAL), was to be found in the sense of a growing need for agencification. Second, it was also evident that ENISA was supposed to be a regulatory agency, as it was and still is called «to be actively involved in the executive function by enacting instruments which help to regulate a specific sector» instead of being «responsible for purely managerial tasks» (COM(2002) 718 FINAL). Finally, the year before ENISA was set up, the framework Regulation for executive agencies (COUNCIL REGULATION (EC) NO 58/2003) clearly established that fixed-term duration is a typical feature of the latter only (CHAMON 2016).

One possible reason for the present and reiterated inconsistency in the system can be drawn out of the uncertain nature of ENISA's legal basis. In fact, the Agency was established having regard to article 114 TFEU (ex 95 TEC), i.e. the Treaty provision which allows the EU legislative power to adopt measures for the approximation of the provisions laid down by law, regulation or administrative action in MSs which have as their object the establishment and functioning of the internal market. It is widely held in literature (OHLER 2006; VETTER 2005; MOK 2006; GUTMAN 2006; RANDAZZO 2007; all cited in CHAMON 2016) that the Agency was to be set up on a different basis or, at least, one including article 352 TFEU and the so-called "subsidiary powers doctrine"[9].

However, when the Court of Justice was called upon to annul ENISA's basic regulation on the basis of the inconsistency with the ratio of article 95 TEC, it departed from the opinion by AG J. Kokott and dismissed case by holding that

phenomenon of EU agencies draws on the previous US experience, similarities between the two should not be overestimated as the american federal governance presents a completely different legal framework (see also CJUE, Case 10-56, *Meroni*).

9 Article 352 TFEU allows the EU to adopt acts which are deemed as necessary to attain objectives laid down by the Treaties when the latter have not provided the powers of action necessary to attain them. However, there are authors who express views of a slightly different persuasion. For instance, CRAIG puts ENISA in the context of the "third wave" or "quasi-regulatory" agencies, i.e. the ones set up in the new millennium, which do not have legal base in art. 352 TFEU due to the turn in the Commission choice to establish new bodies on the basis of particular policy tasks to be performed.

«the establishment of a Community body such as the Agency was an appropriate means of preventing the emergence of disparities likely to create obstacles to the smooth functioning of the internal market in the area» (CJUE, C-217/04, *ENISA,* para. 62; BOUVERESSE 2006; HANSMANN 2006; FABIANO 2006; I. IGLEZAKIS, 2006).

The ruling is at least ambiguous in its reasoning. In fact, it is not evident how the creation of a new body should be regarded per se as a means towards harmonisation. On the contrary, it is quite clear that the non-permanent nature of ENISA played a crucial role in the Court's reasoning (CHAMON 2016). In fact, the EU judges argued that the Agency was given a mandate lasting for a period of five years only and that «the Community legislature considered that before making a decision as to the fate of the Agency it was appropriate to carry out an evaluation of the effectiveness of that Agency and the contribution which it makes to the implementation of the Framework Directive and specific directives» (Case C-217/04, cit., para. 65-67). It thus seems that the Court wanted to suggest that only an effective contribution to the harmonisation of national legislation would make sense of ENISA's very existence. In fact, that was the reason why the Agency had to be set up as a non-permanent body, notwithstanding its regulatory nature. Hence, ENISA is a body correctly established on the basis of the Treaty provision which empowers the EU legislature to harmonise national law only insofar as the Agency is a means to the tasks it was given, i.e. the removal of technical obstacles to the implementation of transnational cybersecurity in the internal market.

However, the mandate of the Agency should now be amended and kept on a fixed-term basis for a number of reasons.

First, it is the opinion of the author that the suitability of a legal basis for the establishment of a new body does not depend on material results performed by the body during its mandate. In fact, the appropriateness of a legal provision and the power it confers on EU institutions with reference to a certain objective are an *a priori* attitude of the norm and thus stay valid regardless of the actual results of the action based on the provision itself.

Second, the legitimacy of ENISA's standing is no longer questioned in

terms of output quality. The Agency has proven to be an example of administrative efficiency, praised by both the general public in the latest public consultation and the European Ombudsman's efficiency prize.

Third, in light of the increasing need for an expertise-based reference point in the field of NIS and cybersecurity, ENISA needs to be given a permanent status also for the sake of the continuity of its work. The issue at stake is even more sensitive if we consider that ENISA is called upon to play an ever greater role while lacking not only an adequate time-frame expectancy but also sufficient budgetary and HR resources[10].

In that respect, the present argument stands in contrast to the *2012 Joint Statement and Common Approach* by the Inter-Institutional Working Group on EU decentralised agencies[11]. In fact, the Statement recommends providing agencies' founding acts with either a sunset clause or a review clause, thus promoting the non-permanent body policy option.

However, it is important to underline that the Statement itself considers the process of closing down an agency to be a solution for bodies that are either underperforming or no longer relevant as a policy option. ENISA does not meet any of those preconditions. On the contrary, as demonstrated above, it is likely that there will be an increasing need for ENISA's service. In addition, a "periodic overall evaluation" envisaged in the Joint Statement (para. 60) would be sufficiently adequate in order to ensure ex-post control and to respond to performance concerns even without the provision of any mandatory sunset clause and, if necessary, to amend ENISA's basic Regulation or close it down accordingly.

Most recently, the European Commission announced the launch of a new proposal for a Regulation on the future of ENISA called the «Cybersecurity Act» (COM/2017/0477 final). As widely envisaged in the present paper and contrary to

10 The mentioned issues have been raised both in the past (see, for instance, EU Agencies Network 2014) and recently (see Euractiv.com) without any responsive echo among the general public.

11 The Inter-Institutional Working Group on EU decentralised agencies (IIWG) was launched by the the European Parliament, Council of the European Union and the European Commission in 2009 as a forum for inter-institutional dialogue.

any of the abovementioned critiques, the proposed article 57(4) explicitly provides that «[t]he Agency shall be established for an *indefinite* period of time starting from […]»[12]. It will now be up to the EU legislator whether to adopt such an act and so grant a more stable future for ENISA. In the meantime, the present landscape offers a great example of how technological innovation comes with spillover effects which are capable to drive administrative and legal reform.

5. Conclusions. A few remarks can now be drawn in conclusion. First, either an amendment to the Agency legal status or the introduction of a permanent mandate seem to be necessary in order for the ENISA's legal framework to comply with the principle of legal consistency among EU regulatory agencies. The European Commission already has taken advantage of the 2018 evaluation process in order to amend the Regulation accordingly. Second, the need for a stable point of reference in cybersecurity governance for the years to come urges the IIWG to review its position with regards to the so-called sunset clause in the drafting of agency frameworks for both the NIS and similar policy areas.

References

A. BOIN - M. BUSUIOC - M. GROENLEER, *Building European Union capacity to manage transboundary crises: Network or lead-agency model?,* in *Regulation & Governance*, Vol . 8, 2014

A. BOUVERESSE, *Bases juridiques autorisant la création d'organismes dotés d'une personnalité juridique propre,* in Europe, nº 203, 2006

M. BOVENS, Analysing and Assessing Accountability: A Conceptual Framework, in *European Law Journal,* Vol. 13, 2007

M. BUSUIOC, *Accountability, Control and Independence: The Case of European Agencies,* in *European Law Journal,* 2009

M. BUSUIOC - M. GROENLEER - J. TRONDAL (eds), *The Agency Phenomenon in the European Union,* Manchester, Manchester University Press, 2010

C. CENCETTI, *Cybersecurity: Unione europea e Italia. Prospettive a confronto,* Roma, Ed. Nuova Cultura, 2014

M. CHAMON, *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration*, Oxford, OUP, 2016

E. CHITI, *Le agenzie europee: unità e decentramento nelle amministrazioni comunitarie*, Padova, Cedam, 2002

12 Enphasis on the word "indefinite" added.

G. CHRISTOU, *The EU's Approach to Cyber Security,* in *EUSC Working Papers,* A/W 2014
P. CRAIG, *EU Administrative Law*, Oxford, OUP, 2012
L. FABIANO, *Articolo 95 TCE e agenzie comunitarie: una nuova pronuncia della Corte di giustizia,* in Diritto pubblico comparato ed europeo, 2006
E. FAHEY*, The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security*, in *European Journal of Risk Regulation (EJRR),*Vol. 5, n. 1, 2014
D. GERADIN - R. MUNOZ - N. PETIT (eds), *Regulation through Agencies in the EU. A New Paradigm for European Governance,* Edward Elgar, Cheltenham, 2005
U. HANSMANN, *Schaffung der Europ. Agentur für Netz- und Informationssicherheit,* in Deutsches Verwaltungsblatt, 2006
C. HARLOW - R. RAWLINGS, *Process and Procedure in EU Administration*, Hart Publishing, Oxford, 2014
I. IGLEZAKIS, *case note*, in Elliniki Epitheorisi Evropaïkou Dikaiou, 2006
G. MAJONE, *The new European agencies: regulation by information*, in *Journal Of European Public Policy,* Vol. 4 , n. 2,1997
B. MCKENNA**,** *ENISA set to join Internet governance debate,* in *Computer Fraud & Security*, Vol. 2004, n. 10, 2004
B. MCKENNA**,** *ENISA surveys evolving threat landscape*, in *Computer Fraud & Security*, Vol. 2013, n. 1, 2013
L. LANGER - F. SKOPIK - P. SMITH - M. KAMMERSTETTER, *From old to new: Assessing cybersecurity risks for an evolving smart grid*, in *Computers & Security,* Vol. 62, Sept. 2016
B. RITTBERGER - A. WONKA, *Agency Governance in the European Union,* in *Journal of European Public Policy,* Vol 18, 2011
J. RUOHONEN - S. HYRYNSALMI - V. LEPPÄNEN, *An outlook on the institutional evolution of the European Union cyber security apparatus*, in *Government Information Quarterly*, Vol. 33, n. 4, October 2016
R. TAUWHARE, *Improving cybersecurity in the European Union: the network and information security Directive*, in *Journal of Internet Law,* Vol. 19, n. 12, 2016

Jurisprudence

Judgment of the Court of 13 June 1958, Case 10-56, *Meroni & Co., Industrie Metallurgiche, società in accomandita semplice v High Authority of the European Coal and Steel Community,* 1958 I-51
Judgment of the Court (Grand Chamber) of 2 May 2006, Case C-217/04, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union. [ENISA],* 2006 I-03771

Legal acts and institutional documents (by date)

Communication from the Commission, *The operating framework for the European Regulatory Agencies*, COM(2002) 718 final, Brussels, 11.12.2002
Council Regulation (EC) No 58/2003 of 19 December 2002, *Statute for executive agencies to be entrusted with certain tasks in the management of Community programmes*, OJ L 11, 16.1.2003
Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004, *establishing the European Network and Information Security Agency,* L77/1, 13.03.2004
Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 *amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency,* 18.10.2011 L 272/1
Council Resolution of 18 December 2009 *on a collaborative European approach to Network and Information Security*, OJ C 321, 29.12.2009

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe (COM/2010/0245 f/2)
Regulation (EU) No 580/2011 of the European Parliament and of The Council of 8 June 2011, *amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration,* 24.6.2011 L 165/3
Joint Statement and Common Approach agreed upon in July 2012 by the Inter-Institutional Working Group on EU decentralised agenzie
Joint communication to the European Parliament, the Council, the European Economic And Social Committee and the Committee Of The Regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013 (JOIN(2013) 1 final)
European Commission, *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union,* Bruxelles, COM(2013) 48 final, 7.2.2013
Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, *concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004*, 18.6.2013 L 165/41
EU Agencies Network, *Position for annual exchange of views between EU agencies and European Parliament Committee on Budgets*, Brussels, 18 July 2014
ENISA, *An evaluation Framework for National Cyber Security Strategies*, November 2014
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on t*he European Agenda on Security*, Strasbourg, 28.4.2015 COM(2015) 185 final
European Commission, *Better Regulation Guidelines*, Staff Working Document, COM(2015) 215 final, Strasbourg, 19.5.2015
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*, COM(2016) 410 final, Brussels, 5.7.2016
Communication from the Commission to the European Parliament, the European Council and the Council, *Seventh progress report towards an effective and genuine Security Union*, Strasbourg, 16.5.2017 COM(2017) 261 final and press release IP/17/1303, 16.5.2017
Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") COM/2017/0477 final

Dati biometrici, firma grafometrica e contratti elettronici. Quali implicazioni per la Cyber Security

di **MARIA ROSARIA LENTI**

Abstract

The purpose of this contribution is to analyze the evolution of the subscription arrangements for the conclusion of the contractual instrument, from electronic signatures to graphometric signatures and biometric data, highlighting the advantages and criticalities of these innovations under the security profile and the prevention and protection measures developed by the Guarantor Authority.

1. Introduzione. La dinamicità della moderna realtà economica e l'avvento della tecnologia hanno rivelato l'esigenza di una rivisitazione delle tradizionali modalità di conclusione dei contratti.

Si è, così, profilata l'ipotesi di abbandonare il supporto cartaceo e di avvalersi dei mezzi informatici, più conformi alla frequenza e alla rapidità degli scambi.

La trasfusione dei moderni standard tecnologici nel settore negoziale ha, però, richiesto un adeguamento delle norme, che già disciplinavano le fasi della formazione, la forma e la prova dei contratti, alle connotazioni degli strumenti elettronici e la creazione di una nuova regolamentazione, che precisasse gli effetti e le modalità di redazione dei negozi telematici.

Dunque il legislatore, nel tentativo di (in)seguire le nuove tecnologie e di trasporle nel diritto, si è trovato ad affrontare un ventaglio di problematiche nuove e del tutto inaspettate, in termini di furto d'identità e di protezione dei dati, e a fare i conti con il complesso funzionamento del mondo digitale,

inesplorato e imprevedibile per il giurista, privo di conoscenze tecniche in merito.

Il presente contributo ha l'obiettivo di analizzare l'evoluzione delle modalità di sottoscrizione dei contratti, dalla firma elettronica alla firma grafometrica e all'utilizzo dei dati biometrici, mettendo in risalto i vantaggi e le criticità di tali novità sotto il profilo della sicurezza e vagliando le misure di prevenzione e di protezione elaborate dall'Autorità Garante per la Protezione dei Dati Personali.

2. Dalla firma olografa alla firma digitale. Nell'ambito del settore documentale, la sottoscrizione autografa di un atto pubblico o di una scrittura privata rappresenta l'ultimo momento della più tradizionale forma di manifestazione di volontà negoziale.

La firma consente di assolvere a tre funzioni. Essa, difatti, vale ad individuare l'autore della sottoscrizione, che, quindi, si assume la responsabilità di quanto dichiarato[1], e ad ingenerare una presunzione *iuris tantum* di accettazione da parte del sottoscrittore del contenuto negoziale.
Per di più ad essa va riconosciuta una valenza probatoria.

Quando il contratto è redatto nella forma dell'atto pubblico, la sottoscrizione suggella l'intervenuto accordo in un atto che ha una forza probatoria privilegiata: soltanto mediante una querela di falso è possibile contestare la provenienza delle volontà negoziali delle parti e l'attestazione del pubblico ufficiale che tali dichiarazioni sono state rese in sua presenza (art. 2700 c.c.).

Se, invece, la sottoscrizione autografa chiude una scrittura privata, quest'ultima fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi ha sottoscritto, soltanto se la firma è autenticata o se la parte contro cui è prodotta la scrittura riconosce la propria sottoscrizione (art. 2702 c.c.).

1 Cass. civ., 2 febbraio 2006, n. 2332, in *Mass. Giur. It.*, 2006; Cass. civ., 16 agosto 2004, n. 15949, in *Mass. Giur. It.*, 2004; Cass. civ., 14 febbraio 2013, n. 3730, in *CED Cassazione*, 2013.

In seguito alla rivoluzione digitale il legislatore ha ritenuto opportuno elaborare una nuova forma di documento, che potesse prescindere dal supporto cartaceo, ma strutturato in modo tale da rispondere ai requisiti di validità formale e di efficacia probatoria e all'esigenza di imputazione dell'atto tradizionale.

I primi interventi hanno riguardato il settore pubblicistico.

L'art. 15 della L. 7 agosto 1990 n. 241 ha previsto l'obbligo per le pubbliche amministrazioni di concludere accordi per la disciplina dello svolgimento di attività di interesse comune, da sottoscrivere, a pena di nullità, con firma digitale, firma elettronica avanzata o altra firma elettronica qualificata. Successivamente l'art. 11 del d.lgs. 12 aprile 2006 n. 163, in tema di affidamento dei lavori pubblici ha prescritto, a pena di nullità, la stipula del contratto con modalità elettroniche; previsione poi ribadita dal d.lgs. 18 aprile 2016 n. 50 in materia di aggiudicazione dei contratti di concessione, appalti pubblici e contratti pubblici relativi a lavori, servizi e forniture[2].

Occorreva affermare questa tendenza, favorevole al modello digitale, anche in campo privatistico.

I vantaggi della stipulazione di un contratto mediante strutture telematiche erano visibili ad occhio nudo.

Innanzitutto il formato digitale accorciava i tempi e i costi non solo di redazione e sottoscrizione, ma anche di trasmissione[3] dell'atto, di registrazione e di pubblicità, riduceva gli spazi e gli oneri di conservazione, e, infine, consentiva una circolazione del documento medesimo con maggiore facilità e immediatezza.

2 Oltre ai comuni vantaggi derivanti dall'utilizzo delle strutture informatiche, il legislatore ha promosso l'impiego di tali supporti per una maggiore trasparenza dell'operato della Pubblica Amministrazione.

3 La scrittura privata non richiede la contestualità dei soggetti sottoscriventi, ma proposta e accettazione possono essere predisposti in momenti e luoghi diversi. In tal caso, il vantaggio apportato dalla fruizione di strutture informatiche, in termini di riduzione dei tempi e dei costi, è ancora più tangibile.

Nel panorama giuridico ha fatto, quindi, ingresso il documento informatico[4], quale rappresentazione informatica di atti, dati e fatti giuridicamente rilevanti[5], su cui può essere apposta una firma elettronica semplice, una firma elettronica qualificata o una firma digitale[6].

Ma quale valore attribuire ad un documento così composto?
E' plausibile affermare che la firma elettronica, in tutte le sue tipologie, permetta di assolvere le tre funzioni, innanzi descritte in materia di firma autografa, vale a dire quella indicativa (dell'autore), dichiarativa (dell'accettazione del contenuto dell'atto) e probatoria?

La firma elettronica, definita dall'art. 1 del D. Lgs. 82/2005 (Codice dell'Amministrazione Digitale, di seguito CAD) come l'insieme dei dati in forma elettronica, allegati o connessi tramite un'associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica, costituisce una forma debole di firma, in quanto non si avvale di meccanismi di autenticazione del firmatario o idonei ad assicurare l'integrità del documento. Dunque essa è liberamente valutabile in giudizio.

La funzione indicativa e quella dichiarativa sono, invece, assolte dalla firma elettronica avanzata, la quale è composta da un insieme di dati in forma elettronica, creati con mezzi sui quali il firmatario conserva un controllo esclusivo e i quali garantiscono l'identificazione e la connessione univoca tra firmatario e documento informatico.

Per quanto attiene, invece, all'aspetto probatorio, la soluzione a tale quesito non poteva non tener conto di un dato immediatamente tangibile di diversità tra firma autografa e firma digitale.

La prima è indissolubilmente legata alla persona del sottoscrittore: se la parte deve apporre la sottoscrizione di propria pugno, deve necessariamente partecipare all'atto, in quanto nessun altro può intervenire per firmare con il suo

4 Il documento informatico risponde alla nozione di documento come mezzo materiale di rappresentazione di atti o fatti, in cui la materialità consiste nella fisicità degli impulsi elettronici impressi sui supporti.
5 E' questa la definizione dell'art. 1 del D.P.R. del 28 dicembre 2000 n 445.
6 La firma digitale costituisce una tipologia della firma elettronica qualificata.

nome e cognome. D'altronde sarebbe facilmente rilevabile la divergenza tra la firma autentica e la firma falsificata.

Diversamente l'apposizione della firma digitale, che è composta da una sequenza alfanumerica crittografica di byte, potrebbe sfuggire alla diretta partecipazione del titolare della stessa. Difatti l'attività di digitazione di dati informatici potrebbe anche essere compiuta da un terzo, senza che vi sia un segno evidente di tale sostituzione, e anche all'insaputa del titolare della firma digitale medesima.

Pertanto il pericolo di un'abusiva apposizione della firma digitale e la inidoneità della firma digitale a provare, in maniera assoluta ed inconfutabile, che il sottoscrivente sia il reale titolare, hanno condotto il legislatore, a riconoscere l'efficacia di mera scrittura privata, ai sensi dell'art. 2702 c.c., al documento sottoscritto con firma avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche che garantiscono l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento (art. 21, secondo comma del CAD)[7]. L'art. 21 succitato ha, quindi, previsto che l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.

Il conferimento al documento informatico del solo effetto della scrittura privata consente al titolare di rifiutare la paternità del documento, dando prova del "furto" di identità digitale, o di sottrazione dei codici identificativi, nonostante le misure di sicurezza adottate ai sensi dell'art. 32 del CAD.

In realtà, il rinvio dell'art. 21 del CAD all'art. 2702 c.c. appare improprio in quanto quest'ultimo articolo riserva al titolare la possibilità di disconoscimento della firma olografa, mentre la firma digitale non pone un problema di autenticità in senso stretto e di formale titolarità. Difatti, la connessione della firma digitale al titolare del dispositivo di firma è certa ed inequivocabile, per cui non è possibile un disconoscimento, ma, in tale ipotesi, emerge un problema di

7 Originariamente, l'art. 6 del D. Lgs. 23 febbraio 2002 n. 10 aveva attribuito al documento sottoscritto con la firma digitale o con altro tipo di firma elettronica avanzata valenza di piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto, vale a dire il valore probatorio di un atto pubblico o di una scrittura privata autenticata.

abusiva appropriazione, data la prospettazione dei pericoli di furto dell'identità digitale e di utilizzo indebito dei dispositivi di firma.

Il legislatore ha, quindi, posto sullo stesso piano due situazioni in realtà intrinsecamente differenti, allo scopo, però, di tutelare, in senso lato, la reale riconducibilità del documento al titolare della firma. Egli ha attribuito ad un soggetto la possibilità di disconoscere la firma recante il suo nome e cognome, apposta su una scrittura privata cartacea, così come ha riconosciuto il potere al titolare di una firma digitale di dimostrare di non aver personalmente apposto e non aver autorizzato nessuno ad apporre la sua firma, escludendo così la paternità del documento medesimo.

Si vengono a delineare le medesime dinamiche esistenti nel mondo analogico.

Sotto il profilo probatorio, il documento informatico corredato da firma digitale, al pari della scrittura privata, rappresenta una fattispecie del tutto contestabile e compromettibile.

Salve le ipotesi di querela di falso, la non ripudiabilità del documento informatico può essere conseguita solo con l'autenticazione della firma digitale medesima o con la redazione dell'atto pubblico informatico.

Difatti, ai sensi dell'art. 25 del CAD, l'autentica delle firme digitali da parte del pubblico ufficiale, oltre a garantire la legittimità del contenuto dell'atto, scagiona ogni ipotesi di illegittima sottrazione del dispositivo di firma, certificando la provenienza della firma medesima da parte dell'effettivo titolare, ed elimina la possibilità di future contestazioni relative alla vigenza dei certificati di firma al momento della sottoscrizione[8], assicurando la validità del certificato di firma nel momento dell'apposizione della firma digitale.

Sia nell'autenticazione delle firme, sia nella redazione di un atto pubblico informatico, il pubblico ufficiale dovrà utilizzare un sistema informatico che renda visibile e verificabile la generazione delle firma digitali sul documento medesimo, dovrà predisporre un documento non falsificabile e statico e che

8 La conseguenza è rilevante dato che l'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso, equivale a mancata sottoscrizione.

consenta di rilevare e registrare ciò che può essere stato aggiunto dopo le sottoscrizioni[9], garantendo così la non modificabilità del documento e la tutela della volontà delle parti.

3. Dalla firma digitale alla firma grafo metrica e all'utilizzo dei dati biometrici. La sottoscrizione di un contratto con firma digitale presenta, però, degli inconvenienti.

In primo luogo, è necessario che ogni parte del contratto abbia acquistato il dispositivo di firma, sostenendo i relativi costi, da un'autorità di certificazione abilitata al rilascio e che essa sia ancora valida. L'acquisizione comporta, inoltre, per il titolare, l'adempimento di oneri di custodia relativamente al dispositivo di firma e il pin di accesso. La realtà è che la firma digitale è diffusa in ambito professionale e aziendale, ma è ancora avvertita da molti come uno strumento non indispensabile e di complessa fruibilità.

In secondo luogo la sottoscrizione di un contratto con firma digitale richiede l' interoperabilità tra i vari sistemi di firma digitale. Spesso, però, il sistema operativo utilizzato non adopera lo stesso linguaggio dei software connessi alle varie firme digitali, non riconoscendo detti sistemi di firma e impedendo, così, il perfezionamento del contratto.

In terzo luogo, la mancata percezione da parte dei titolari della firma digitale come propria sottoscrizione ha indotto gli stessi, più o meno consapevolmente, a concedere a terzi l'utilizzo della smart card e del relativo codice, determinando la crescita dei casi di utilizzazione indebita.

Tali criticità hanno costituito il terreno fertile per la nascita e la diffusione della firma grafometrica.

La firma grafometrica consiste nella trasposizione della propria sottoscrizione olografa su un dispositivo elettronico (tablet). Essa può valere non solo a riprodurre la firma del sottoscrivente come se il tablet fosse un foglio di carta, ma anche a rivelare ulteriori connotati relativi alla persona che

9 Tale obiettivo viene conseguito mediante l' implementazione del pdf/a, parte dello standard ISO 32000.

sottoscrive. I dispositivi, infatti, sono in grado di acquisire un insieme di altri dati biometrici di natura identificativa, rientranti nella categoria delle caratteristiche biometriche comportamentali[10], vale a dire la velocità di tracciamento, l'accelerazione, la pressione, le inclinazioni, i salti in volo.

I dati biometrici[11] consentono in modo univoco di individuare il titolare, evidenziando la connessione necessaria e universale tra corpo e identità.

Per tali ragioni, originariamente, la firma grafometrica era stata introdotta per accompagnare la firma digitale, al fine di aumentarne il livello di sicurezza; in un secondo momento, essa è stata considerata come autonomo strumento di identificazione o di sottoscrizione.

La firma grafometrica si mostra come un mezzo più vantaggioso, in termini di comodità e immediatezza, rispetto alla firma digitale.

Essa consente con più facilità di concludere un contratto con strumenti digitali, perché non richiede la titolarità di alcun dispositivo di firma, non può comportare problemi di comunicazione tra i sistemi informatici e non può dar luogo a fenomeni di utilizzo dei dispositivi di firma da parte di terzi.

Inoltre la stretta affinità con la firma autografa favorisce la diffusione di tale modalità di conclusione di contratti.

Per rintracciare il valore probatorio della firma grafometrica è necessario individuare la sua natura giuridica.

---

10 Nella biometria è possibile distinguere due categorie: la biometria fisica, basata sulla estrazione di dati da caratteristiche anatomiche del soggetto, quali l'iride, l'impronta digitale, le caratteristiche del volto, e la biometria comportamentale, basata su elementi attinenti al comportamento di uno specifico soggetto, quali l'emissione della voce e l'apposizione di una firma: *Linee guida in materia di riconoscimento biometrico e firma grafometrica*, Allegato A al Provvedimento del Garante del 12 novembre 2014.

11 I dati biometrici sono definiti dal Regolamento 2016/679 del Parlamento europeo e del Consiglio come «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o ne confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici». Tra questi si ricorda l'impronta digitale, la topografia della mano o il riconoscimento dell'iride. L'utilizzo dei dati biometrici è oggi molto diffuso non solo per la sottoscrizione di documenti informatici, ma anche per l'accertamento dell'identità personale, per il controllo di accessi a locali o aree, per l'attivazione di dispositivi elettronici. La questione ha suscitato anche l'interesse del *Working Party Article 29*, un organismo consultivo e indipendente di rilevanza comunitaria, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione.

Senza dubbio, essa costituisce una tipologia di firma elettronica, quale insieme dei dati in forma elettronica, allegati oppure connessi ad altri dati elettronici.

La firma *de qua* ha, tuttavia, la possibilità di potenziare il suo valore giuridico e l'effetto probatorio, qualificandosi come firma elettronica avanzata. In tal caso sarà determinante che le modalità di generazione, apposizione e verifica delle firme rispettino i requisiti soggettivi ed oggettivi richiesti per le firme avanzate. Alla base dell'acquisizione della firma biometrica vi dovrà essere un processo che garantisca l'identificazione univoca del firmatario e l'integrità del documento, anche nella fase di conservazione.

Vi è quindi una differenza, sotto il profilo probatorio, tra la firma grafometrica quale mero tratto grafico apposto su un tablet, senza che vi sia alcuna registrazione di dati biometrici, e la firma grafometrica su dispositivo che ne conserva ed elabora i dati, e ne garantisce la riconducibilità al titolare.

Nel primo caso, essa sarà liberamente valutabile in giudizio; nel secondo caso, essa farà piena prova, fino a querela di falso, della provenienza della dichiarazione, salvo il disconoscimento.

In ogni caso, in entrambe le ipotesi, l'accertamento della veridicità della sottoscrizione sarà più simile a quello compiuto in caso di firma autografa. Difatti il recupero del segno grafico comporterà anche il ritorno alle tradizionali metodologie di verifica dell'autenticità della firma e il perito potrà inoltre usufruire delle ulteriori informazioni fornite dai dati biometrici scaturenti direttamente dalla firma biometrica.

4. Le minacce cyber derivanti dall'uso della firma grafometrica. L'utilizzo della firma grafometrica e dei dati biometrici pone degli evidenti pericoli di tutela della riservatezza dei dati personali.

Non a caso l'art. 31 del Codice in materia di protezione dei dati personali dispone che detti dati, oggetto di trattamento, devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in

modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Purtroppo l'acquisizione non consentita di dati biometrici non è mai fine a se stessa, ma strumentale al compimento di ulteriori illeciti. Tra questi, appaiono significativi il trattamento illecito di detti dati per fini discriminatori o di controllo sociale, il furto d'identità digitale, la falsificazione della firma biometrica.

4.1 Il trattamento illecito dei dati biometrici. I dati biometrici sono degli identificatori universali, legati univocamente ad un determinato soggetto. Alcuni di essi denotano lo stato di salute, l'etnia di appartenenza, le caratteristiche fisiche di un utente.

La raccolta di detti dati potrebbe avvenire per realizzare degli scopi non dichiarati e illegittimi. Difatti, in assenza di misure preventive e di controllo, nulla impedisce ad istituzioni e privati di acquisire i dati biometrici e di combinarli con altri dati sensibili, ricavati da banche dati differenti, al fine di tracciare un profilo completo del soggetto di riferimento.

La conoscenza degli elementi fisici e comportamentali rappresenterebbe un'arma pericolosa nelle mani dei titolari del trattamento, i quali potrebbero attuare politiche di discriminazione o di controllo e condizionamento indiretto. A livello macroscopico, sarebbe possibile seguire gli spostamenti degli utenti in via generalizzata, compromettendone la privacy.

Paradossalmente, la biometria perderebbe la sua funzione di risorsa per la sicurezza semplificata e si tradurrebbe in una forma di controllo da parte di terzi.

4.2 Il furto d'identità digitale. Il termine di identità comprende due accezioni: una che attiene intimamente al soggetto e l'altra connessa all'appartenenza dell'individuo alla collettività.

Si fa riferimento, quindi, sia alla qualità del soggetto che, in termini oggettivi, consente la sua individuazione, sia alla proiezione sociale della sua personalità[12].

Se l'identità personale ha tale doppia valenza, è chiaro che anche l'interesse sotteso alla sua tutela non può che essere doppio. Il legislatore, difatti, intende garantire non solo il diritto del soggetto titolare di essere riconosciuto, ma anche l'interesse dei terzi alla corretta identificazione dei consociati[13]. Si vuole salvaguardare la persona e la pubblica fede, la quale può essere violata da inganni relativi alla vera essenza della persona e delle sue azioni.

Ma se per diritto all' identità si intende l'interesse del soggetto ad essere rappresentato nella vita di relazione con i suoi connotati, a non veder alterato il proprio patrimonio intellettuale, religioso, ideologico, a non veder disconosciuta la paternità delle proprie azioni o a non vedersi attribuita la titolarità di azioni altrui, allora non può non essere ricompresa, nella nozione di identità personale, anche quella digitale, quale manifestazione del soggetto nelle attività informatiche e nel web.

Anche l'identità digitale presenta un doppio volto: essa può manifestarsi nella rappresentazione sul web di un soggetto e può ridursi all'insieme dei codici elettronici che consentono l'identificazione del soggetto nei sistemi informatici, in virtù di una correlazione tra tali cifre e l'utente[14]. I codici elettronici

12 La giurisprudenza ha ricondotto il diritto all'identità nella categoria dei diritti fondamentali, come tutelati dall'art. 2 della Costituzione, espressione del libero e integrale svolgimento della persona umana: Cass. civ., 22 giugno 1985, n. 3769, in *CED Cassazione;* Cass. civ., 7 febbraio 1996, n. 978, in *Foro it.*, 1996, c. 1253.

13 In realtà la nozione di identità personale si è, nel tempo, riempita di significato. Originariamente il bene tutelato era quello della individualità, ai fini di una corretta identificazione del soggetto quale autore di una determinata prestazione o attività: la tutela dei diritti soggettivi, protetti legislativamente dalle *property rules* (cfr. art. 7 c.c. e art. 10 c.c.; in Germania par. 12 BGB), era rimessa all'intervento autonomo dei singoli. Successivamente, acquisisce rilevanza la dimensione sociale della personalità e la sua esplicazione nei rapporti con i terzi. L'ordinamento si attribuisce un ruolo di controllo, per assicurare il rispetto dell'identità di ciascun soggetto.

14 La rilevanza dell'identificazione digitale è evidente anche in ambito europeo. Il recente Regolamento EIDAS (*Electronic, Identification, Authentication, Signature)* promuove un mercato unico digitale, mediante la creazione di un quadro giuridico uniforme per le firme elettroniche, i documenti elettronici e i servizi relativi ai certificati di autenticazione dei siti web, pur lasciando ogni Paese libero di creare il proprio sistema di identificazione elettronica. L'Agenda Digitale del

possono consistere in parole chiave (password), componenti biologiche (impronta digitale o vocale, riconoscimento del volto, iride) o elettroniche connesse a dispositivi (smart card, tessere magnetiche).

Il furto di identità digitale si configura, quindi, come l'appropriazione da parte di soggetti non legittimati degli elementi che consentono sul web il riconoscimento del soggetto, nonché dei suoi codici elettronici e delle sue caratteristiche biometriche.

Differenti possono essere le modalità attraverso cui si realizza il furto d'identità: si possono captare informazioni personali mediante l'*hackeraggio* dei sistemi telematici, attraverso condotte fraudolenti (*phishing*), quali l'invio di e-mail da fittizi istituti bancari, o mediante estrapolazione di dati da documenti smarriti.

Anche in tali casi, il danno è cagionato non solo al titolare dei dati, che perde il suo profilo in rete e in maniera definitiva, in quanto i dati denotano l'utente in maniera esclusiva, ma anche alla collettività, che non ha più alcuno strumento per individuare tale soggetto e il suo operato.

La tutela dell'identità digitale è sancita dall'art. 494 c.p. che sanziona con la reclusione fino ad un anno la condotta di chi, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, stato, qualità cui la legge attribuisce un effetto giuridico.

La Suprema Corte ha specificato che il reato di sostituzione di persona ai sensi dell'art. 494 c.p. può essere compiuto in rete, mediante l'indebito utilizzo degli account personali[15].

E' evidente che l'oggetto del furto può essere rappresentato da qualsiasi connotazione identificativa, non solo da password e codici utenti, ma anche dall'insieme dei dati biometrici e degli elementi sottesi alla firma grafometrica.

Governo Italiano ha, invece, introdotto lo SPID, vale a dire un sistema che consentirà di realizzare la propria identità digitale, mediante una corrispondenza biunivoca tra soggetto e dati personali, i quali potranno essere utilizzati per accedere automaticamente ad altre piattaforme web.

15 Cass. pen., 14 dicembre 2007, n. 46674, in *Dir. Internet,* 2008, 3, 249; Cass. pen., 3 aprile 2012, n. 12479, in *CED Cassazione*, 2012.

Le conseguenze dannose si moltiplicano quando il furto d'identità digitale diviene funzionale al compimento di altri reati, generalmente contro il patrimonio, o costituisce una forma di aggravante di altri illeciti penali[16].

E' il caso del reato di frode informatica, che può essere "accompagnato", ai sensi dell'art. 640 *ter* c.p., dal furto o dall'indebito utilizzo dell'identità digitale, integrando la fattispecie del concorso formale tra reati.

Il *phishing*, ad esempio, costituisce una tipologia di frode informatica e si realizza mediante la sottrazione dei dati elettronici e biometrici, correlati, ad esempio, ai servizi di *home banking*, da parte degli autori dell'illecito, i quali, in un secondo momento, li utilizzano per realizzare spostamenti di denaro e accrediti non autorizzati. Si può realizzare una frode informatica anche mediante l'intercettazione dei flussi dei dati della vittima e il reindirizzamento automatico su siti web fraudolenti, simili a quelli da lei abitualmente consultati per effettuare acquisti *on line*.

Ricorre il concorso di reati anche tra il delitto di cui all'art. 494 c.p. e l'illecito di cui all'art. 615 *ter* c.p., consistente nell'accesso abusivo in un sistema informatico protetto da misure di sicurezza.

4.3 La falsificazione della firma biometrica. L'utilizzo di dispositivi che raccolgono i dati biometrici dovrebbe avvenire in modo tale da escludere che dal modello acquisito si possa ricavare il campione biometrico.

Il processo di raccolta dei dati dovrebbe, infatti, essere unico e irreversibile.

Il rischio di una registrazione e successiva elaborazione dei dati è che si dia luogo ad una riproduzione non autorizzata dei dati biometrici, utilizzabili al di fuori del contesto nel quale sono stati legittimamente raccolti.

Oltre al rischio della riproduzione, vi è anche quello della falsificazione biometrica, vale a dire della creazione di caratteristiche biometriche artificiali a

16 Non meno diffuse sono le fattispecie aventi ad oggetto condotte prodromiche alla sostituzione di persona con furto d'identità: si fa riferimento alla diffusione di programmi informatici (virus) aventi come scopo quello di alterare il sistema informatico, ad esempio acquisendo le credenziali di accesso, di cui all'art. 615 *quinquies* c.p.

partire da elementi biometrici esistenti. Se dalla manipolazione delle caratteristiche biometriche registrate è possibile ottenere nuove identità digitali, è evidente il pericolo del compimento di truffe e scambi d'identità.

5 Le misure preventive. Di fronte alle minacce di furto d'identità e di trattamento illecito dei dati biometrici, si è ravvisata la necessità della predisposizione di una regolamentazione per l'adozione di misure di protezione e di un apparato cautelare.

L'Autorità Garante per la Protezione dei Dati Personali ha emanato delle linee guida in materia di riconoscimento biometrico e firma grafometrica, in allegato al Provvedimento del 12 novembre 2014, in cui ha tracciato un quadro uniforme di riferimento per l'adozione di strumenti tecnologici nel rispetto dei principi di legittimità stabiliti dal Codice e degli standard di sicurezza.

Al fine di impedire che il trattamento dei dati biometrici possa tradursi in una ingerenza eccessiva ed ingiustificata, l'Autorità ha prescritto il rispetto dei criteri di liceità, necessità, finalità e proporzionalità.

La liceità del trattamento da parte di operatori privati implica il preventivo consenso informato dell'interessato, sempre revocabile e libero da qualsiasi condizionamento, manifestato in forma libera ed espressa[17]. Ai sensi dell'art. 13 del Codice, l'informativa deve specificare le finalità perseguite, le modalità di trattamento e i tempi di conservazione dei dati, la natura obbligatoria o facoltativa del conferimento dei dati e la possibilità di avvalersi di procedure alternative, i soggetti ai quali i dati personali possono essere comunicati.
Se il dispositivo è nella esclusiva disponibilità dell'interessato, l'informativa deve riguardare anche la custodia e gli adempimenti conseguenti al suo smarrimento, alla sottrazione e al malfunzionamento.

La necessità del trattamento comporta che la finalità indicata non è conseguibile in via anonima, ma richiede inevitabilmente l'identificazione

17 Il consenso non è richiesto nei casi in cui il Garante non lo ritenga opportuno, in virtù della prevalenza dell'interesse del titolare del trattamento, con apposito provvedimento.

dell'interessato. L'utilizzazione dei dati personali biometrici è quindi imprescindibile.

Il trattamento dei dati biometrici è, inoltre, ammesso solo per le finalità comunicate: non è possibile estrarre dati ulteriori rispetto a quelli necessari per conseguire gli scopi menzionati, né utilizzare i dati registrati lecitamente per operazioni di trattamento incompatibili con quelle consentite.

La raccolta dei dati biometrici è incentrata sul principio di minimizzazione, per cui non è consentita l'acquisizione di dati non pertinenti e ulteriori rispetto a quelli essenziali per le finalità da perseguire.

In secondo luogo, l'Autorità ha imposto una serie di adempimenti giuridici prima dell'inizio del trattamento. Difatti essa richiede al titolare del trattamento dei dati biometrici[18] un'apposita notifica al Garante e, per il trattamento di dati diversi da quelli sensibili e giudiziari, che può cagionare la lesione dei diritti e delle libertà fondamentali, la presentazione di un'apposita richiesta di verifica preliminare, con indicazione dell'analisi dei rischi e le modalità con cui intende garantire il rispetto delle misure di carattere generale, degli adempimenti giuridici e delle misure di sicurezza. Il Garante può prescrivere misure e accorgimenti specifici per consentire il corretto utilizzo dei dati.

L'Autorità ha, però, individuato delle tipologie di trattamento meno rischiose, in relazione alla tipologia dei dati trattati, alle finalità perseguite e le misure di sicurezza adottabili, per le quali ha escluso la necessità della verifica preventiva, imponendo, tuttavia, anche per tali trattamenti, l'adozione di tutti gli accorgimenti essenziali per garantirne la sicurezza, il rispetto dei presupposti di legittimità imposti dal Codice e l'obbligo di notifica al Garante e di informativa all'utente.

In tale categoria di trattamenti esenti, è presente quello relativo all'apposizione della firma grafometrica.

Il Provvedimento in tema di biometria dell'Autorità Garante del 12 novembre 2014 esclude la necessità della verifica preliminare per l'utilizzo di

18 Ai sensi dell'art. 37 del Codice in materia di protezione dei dati personali, sono escluse determinate categorie di soggetti in ragione dell'attività svolta.

sistemi di firma grafometrica, ma solo se essi posseggono i connotati del meccanismo della firma elettronica avanzata.

Il sistema di firma grafometrica deve, cioè, apportare le medesime garanzie della firma elettronica avanzata, vale a dire deve assicurare l'autenticità e l'integrità dei documenti e tutelare i dati dai rischi di furto e tentativi di frode.

A tal fine, sarà necessario, preliminarmente, identificare il firmatario, utilizzare dispositivi che non conservino i dati biometrici raccolti, ma siano programmati in modo tale che essi vengano cancellati automaticamente una volta completata la sottoscrizione, pur garantendo la memorizzazione degli stessi all'interno dei documenti informatici, e sarà essenziale prevedere sistemi alternativi di sottoscrizione non basati sulla disposizione di dati biometrici.

Anche la redazione degli atti pubblici e le autentiche delle scritture private con firma grafometrica è ormai ammessa, in seguito al Provvedimento dell'Autorità Garante del 25 novembre 2015. Il sistema predisposto dai pubblici ufficiali, come verificato dall'Autorità, permette che i dati biometrici relativi alla sottoscrizione (posizione, pressione, inclinazione, velocità) vengano, unitamente al tratto grafico della firma, acquisiti dal documento informatico, per poi essere completamente cancellati dai dispositivi. Anche in tali ipotesi, configurandosi un trattamento di dati sensibili, non si potrà prescindere dall'informazione preventiva ai sottoscriventi, dalla presenza di sistemi alternativi di sottoscrizione e dal consenso al trattamento dei dati.

6. Note conclusive. Il passaggio dalla firma elettronica alla firma grafometrica mette in evidenza come il processo di dematerializzazione del corpo sia stato posto a servizio della conclusione dei negozi giuridici.

I dati biometrici hanno una forte capacità distintiva, ma il legame corpo-informazione pone delle implicazioni rilevanti per la *cybersecurity*. I rischi di frode informatica, di furto d'identità nonché di trattamento illecito dei dati sono già stati analizzati dall'Autorità Garante per la Protezione dei Dati Personali. Tuttavia, in una realtà complessa come quella digitale, le fattispecie criminose e

le relative modalità di attuazione possono assumere sempre nuovi contorni. Ecco perché appare opportuno che i fenomeni connessi all'uso dei dati elettronici e biometrici siano costantemente sotto osservazione, in modo tale da elaborare tempestivamente, qualora fosse opportuno, una linea difensiva e da prevenire la reiterazione degli illeciti, predisponendo adeguate misure di prevenzione.

Riferimenti bibliografici

G. BAVETTA, voce *Identità (diritto alla)*, in *Enc. dir.,* vol. XIX, Giuffrè Editore, Milano, 1970.
C. M. BIANCA, *Diritto civile*, *Il contratto*, Giuffrè Editore, Milano, 2000.
F. CAJANI, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013 n. 93*, in *Cass. pen*., 3, 2014.
B. CARPINO, voce *Scrittura privata*, in *Enc. dir.*, vol. XLI, Giuffrè Editore, Milano, 1989.
P. CIPOLLA, *Social network, furto d'identità e reati contro il patrimonio*, in *Giur. merito*, 12, 2012.
R. CLARIZIA, *Informatica e conclusione del contratto*, Giuffrè Editore, Milano, 1985.
F. COCUCCIO, *Il diritto all'identità personale e l'identità "digitale"*, in *Dir. famiglia*, 3, 2016.
CONSIGLIO NAZIONALE DEL NOTARIATO, Studio n. 3- 2006 /IG, *Codice dell'amministrazione digitale, firme elettroniche e attività notarile*, (est. M. Nastri), in *Studi e Materiali*, 2006.
L. CUOMO, *Profili giuridici del trattamento biometrico dei dati,* in *Riv. it. med. leg.*, 1, 2014.
F. DELL'AVERSANA, *Documento e firme elettroniche: dal digitale alla grafometria*, Notartel, Roma, 2016.
G. FALCO, voce *Identità personale*, in *Nuovo Dig. it.*, vol. VI, Utet, Torino, 1938.
R. GENGHINI, *Atti pubblici in forma digitale*, in L. GENGHINI, *La forma degli atti notarili*, Cedam, Padova, 2010.
A. GENTILI, *I documenti informatici: validità ed efficacia probatoria*, in *Dir. internet*, 2006, 3.
G. GIACOBBE, *L'identità personale tra dottrina e giurisprudenza. Diritto sostanziale e strumenti di tutela*, in AA.VV., *La lesione dell'identità personale e il danno non patrimoniale*, Giuffrè Editore, Milano, 1985.
G. RESTA, *Identità personale e identità digitale*, in *Dir. informatica*, 3, 2007.
B. SANTACROCE, *Dalla firma digitale alla firma biometrica: quadro giuridico di riferimento per l'applicazione dei nuovi dispositivi di firma,* in P. RIDOLFI (a cura di), *Il nuovo CAD. Commenti e prospettive. Atti del Convegno dell'8 luglio 2011. Roma, Accademia dei Lincei*, Fondazione Siav Academy, Rubano, 2011.
A. TORRENTE - P. SCHLESINGER, *Manuale di diritto privato*, Giuffrè Editore, Torino, 2015

Cybersecurity, (auto)regolazione e governance del rischio. Quid de iure poenali?

di **LUCA D'AGOSTINO**

SOMMARIO: **1.** DALLA *CYBERLAW* ALLA *CYBERSECURITY* – **1.1.** UNA DEFINIZIONE NORMATIVA – **2.** *CYBER-RISK* E DIRITTO PENALE – **3.** IL RUOLO DELL'AUTODISCIPLINA E DELLA *COMPLIANCE* NEL SETTORE DELLA PROTEZIONE CIBERNETICA E DELLA SICUREZZA DELLE INFORMAZIONI: RIFLESSI IN TERMINI DI RESPONSABILITÀ PENALE – **4.** LA DIRETTIVA C.D. *NIS* E LE PROSPETTIVE DI TUTELA PENALE – **5.** CONCLUSIONI.

Abstract

The enactment of directive 2016/1148/UE concerning *"measures for a high common level of security of network and information systems across the Union"* raised the necessity of the implementation of cybersecurity national strategies, imposing risk prevention duties for operators of essential services and digital service providers, and, in case of violation, effective, proportionate and dissuasive penalties against the obliged professionals.
Starting from the arrangement of a legal definition of cybersecurity, after analysing the impact of self-regulation on individual criminal liability, the Author evaluates the new Directive impact on corporate cyber-risk compliance duties, and the emergent liabilities for failure to adopt organizational and technical measures.

1. Dalla cyberlaw alla cybersecurity. I nuovi mezzi di comunicazione e di informazione manifestano in modo sempre più intenso la dimensione "pervasiva" e "globalizzante" (PICOTTI, 2012) del cyberspazio. *Internet* è da sempre considerato un fattore di garanzia e libertà per gli utenti del mondo digitale. Ma nella moderna società dell'informazione esso rappresenta anche un indubbio fattore di rischio per i diritti fondamentali degli individui.

La dicotomia in parola è stata metaforicamente svelata da un compianto Maestro, la cui parole tornano sonore alla mente. *«La rete […] porta con sé anche un'impostazione, più che ideologica, mitologica, che sembra evocare la lancia di Achille e quella di Parsifal, armi capaci di offendere e guarire";* una mitologia che però viene smentita *"da una realtà nella quale non solo Internet è variamente oggetto di regolazione, ma soprattutto conosce violazioni continue di quello statuto di libertà che si riteneva poter essere affidato alla propria, esclusiva virtù salvifica»* (RODOTÀ, 2010).

La regolazione della rete viene attuata mediante la *cyberlaw* (ZICCARDI, 2011) che, in senso lato, viene intesa come il complesso di disposizioni che disciplinano il rapporto tra utenti del mondo digitale al fine di proteggere interessi di primaria importanza come la personalità individuale, la riservatezza delle comunicazioni, la confidenzialità delle informazioni, i dati personali, il diritto d'autore.

Negli ultimi anni la *ITC policy* internazionale si è evoluta in senso "funzionalistico", abbandonando l'idea di un intervento statico e strettamente regolatorio – e quindi la *cyberlaw* nel senso sopra richiamato – in favore di un approccio più "eclettico" e dinamico di tutela. La diffusione del concetto di *cybersecurity* riflette al contempo un fenomeno culturale e un'esigenza della moderna società dell'informazione; lungi dal poter essere ridotta a mero valore di principio, la *cybersecurity* è la risposta "sociale" alla crescente informatizzazione dei processi comunicativi e dei rapporti economici e, con essi, all'aumento del rischio di *cybercrime*. Le statistiche più recenti evidenziano come la criminalità informatica abbia assunto dimensioni draconiane, destinate ad una ulteriore superfetazione in difetto di adeguate misure di prevenzione (SEVERINO, 2017)[1].

1.1 Una definizione normativa. La nota distintiva di questa nuova materia è indubbiamente la trasversalità[2] che la caratterizza.

L'attuazione di un elevato *standard* di sicurezza informatica, specie ove riferito a organizzazioni complesse, richiede una sinergia di competenze di carattere tecnico, economico, giuridico. Si può quindi affermare che la

1 Le statistiche diffuse dal *World Economic Forum* hanno stimato il costo globale della criminalità informatica in 445 miliardi di dollari all'anno, e che, in mancanza di efficaci strategie difensive e preventive nel 2020 le perdite economiche causate dalla criminalità informatica potrebbero arrivare fino a 3.000 miliardi di dollari. Cfr. Consorzio Interuniversitario per l'informatica (CINI) nel documento *Il futuro della Cybersecurity in Italia*, ottobre 2015, p. 2.

2 In questo senso il *Rapporto CLUSIT* (Associazione Italiana per la sicurezza informatica) per l'anno 2016, p. 12 che definisce la *cybersecurity* come *"il gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti […] costruite negli anni a partire da esigenze di compliance".* Il documento è disponibile in *open access* sul portale dell'Associazione al seguente collegamento:
https://clusit.it/wp-content/uploads/download/Rapporto_Clusit%202016.pdf

cybersecurity, condividendo il metodo di ciascuna delle scienze che la riguardano (CARCATERRA, 2011), sia una scienza derivata[3]; in quanto tale essa avrà una definizione propria e obiettivi specifici per ciascun settore di riferimento.

Ciò che interessa, ai nostri fini, è tracciare una definizione valida sul piano giuridico, che possa essere assunta a premessa maggiore del ragionamento sui possibili risvolti penalistici della *cyber-governance*. Il terreno è reso scivoloso dall'assenza di una caratterizzazione, a livello legislativo, della materia. Soltanto negli ultimi anni il legislatore ha cominciato a muovere i primi passi nel settore della "protezione cibernetica" e della "sicurezza informatica"[4] mediante interventi a carattere generale e di natura programmatica. Venendo ai tempi più recenti, l'emanazione della Direttiva 2016/1148/UE (di seguito, Direttiva NIS), rende imminente una organica rivisitazione legislativa e l'adozione di un Piano Nazionale di sicurezza informatica; l'intervento riformatore offrirà l'occasione per una più compiuta definizione normativa della *cybersecurity*. Allo stato attuale essa può essere definita come quella scienza *«che consente a una entità (ad esempio, organizzazione, cittadino, nazione ecc.) la protezione dei propri asset fisici e la confindezialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyber space»*[5]*.*

3 Si assume a base la nozione sociologica di scienza come astrazione di un insieme di cognizioni in un insieme di concetti elaborati attraverso un metodo. Se, sulla scorta di tale definizione, si considerano "scienze" l'informatica, l'economia e il diritto, non vi è dubbio che la *cybersecurity* condividerà anch'essa la medesima natura: essa è quindi una scienza derivata, caratterizzata da un metodo 'eclettico' e condiviso; un metodo che si fonda tanto sulle leggi positive, quanto su quelle della logica e della tecnica.

4 Il riferimento è al Piano Nazionale per la protezione cibernetica e la sicurezza informatica, approvato dal Governo nel dicembre 2013 e disponibile sul sito *internet* istituzionale dell'AgID *http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/piano-nazionale-cyber_0.pdf*

5 Così il *Framework Nazionale di Cybersecurity*, adottato dal CIS (*Cyber intelligence and information security*) dell'Università La Sapienza di Roma e dal CINI (Consorzio interuniversitario nazionale per l'informatica), con la collaborazione dell'Agenzia per l'Italia Digitale, dell'Autorità Garante per la protezione dei dati personali e il Ministero dello Sviluppo Economico; il documento è disponibile sul sito internet del Governo https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/un-framework-nazionale-per-la-cyber-security.html.

Per la precisione, il *Framework Nazionale* definisce la *cybersecurity* come "pratica", al quale abbiamo sostituito, per le ragioni anzidette, l'appellativo "scienza".

2. Cyber risk e diritto penale. La definizione contenuta nel Framework nazionale appare estremamente pertinente per una riflessione sui possibili riflessi della *cybersecurity* sul piano del diritto penale.

Anzitutto, essa focalizza l'attenzione sulle oggettività giuridiche rilevanti, quali la tutela degli *asset* fisici, delle confidenzialità e dell'integrità/disponibilità delle informazioni. Ciò, dal punto di vista del penalista, è indicativo della diversificazione dei beni protetti e, quindi, dei titoli di reato da considerare.

In secondo luogo, la definizione fa espresso riferimento alle minacce che derivano dal cyberspazio, mettendo in luce il rapporto "genetico" di causa-effetto esistente tra *cybercrime* e *cybersecurity*.

Detto rapporto, tuttavia, non si esaurisce nella sola derivazione di quest'ultimo dalla prima, anzi può essere considerato *in fieri*, nel senso che la regolazione pubblica del settore della sicurezza informatica incide sull'estensione di alcune fattispecie di reato e, sotto certi aspetti, apre nuovi orizzonti di criminalizzazione. Viene quindi in rilievo il concetto di *cyber-risk* sul quale l'interprete è chiamato a riflettere per analizzare i possibili riflessi della regolazione sul piano della responsabilità. Sotto questo aspetto, si deve rimarcare la crescente importanza che l'autoregolazione societaria assume nel contesto della *governance* del suddetto rischio

Non si deve infatti dimenticare che, da un punto di vista economico-istituzionale, la *cybersecurity* origina da esigenze di *compliance* a partire da strumenti propri della sicurezza informatica "tradizionale"[6]; per questo motivo anche il profilo l'autodisciplina riveste un ruolo fondamentale nell'implementazione di un *standard* elevato di sicurezza.

Sul piano teorico, quindi, il panorama normativo attuale non consente di delineare una autonoma nozione di *diritto penale della sicurezza informatica* al pari di altre branche (diritto penale dell'economia, del lavoro, delle biotecnologie, dell'ambiente). Ciascuna di queste è caratterizzata dalla presenza di fattispecie penali "di chiusura" di un sottosistema normativo (o più

6 Cfr. *Rapporto CLUSIT* per l'anno 2016, *cit.* p. 12

sottosistemi normativi integrati) e delle regole proprie del settore[7]. La sicurezza informatica – almeno *de lege lata* – non gode di un tessuto normativo organico e, tantomeno, di disposizioni incriminatrici che strettamente la riguardano. Ma pur negando l'esistenza di un autonomo sottosistema, la *cybersecurity* conserva comunque una incidenza indiretta sul piano del diritto penale. L'imposizione di determinati obblighi di protezione e la fissazione di un determinato *standard* di sicurezza diviene rilevante per l'integrazione di alcuni elementi qualificanti (es. il concetto normativo di colpa o di obbligo impeditivo) ovvero per la configurabilità di fattispecie penali appartenenti a settori "contigui" (es. gli illeciti in materia di trattamento dei dati personali; i delitti in materia di rivelazione dei segreti).

Inoltre – esaminando la questione *de lege ferenda* – sembra che la *cybersecurity* sia prossima ad essere riconosciuta da una fonte di rango primario per effetto del recepimento della Direttiva *NIS*; ciò potrebbe aprire nuovi ed importanti scenari d'interesse per il penalista.

3. Il ruolo dell'autodisciplina e della compliane nel settore della protezione cibernetica e della sicurezza delle informazioni: riflessi in termini di responsabilità penale. La *compliance* della sicurezza informatica assume notevole importanza sul piano della responsabilità individuale[8].

Dal punto di vista semantico essa viene definita come *«aderenza alle norme e alle prescrizioni di autoregolamentazione»*[9]*.* La *compliance* si fonda

7 Così, ad esempio, gli illeciti contravvenzionali previsti dal D. Lgs. n. 81/2008 costituiscono il corredo sanzionatorio per la violazione delle disposizioni del sistema prevenzionistico degli infortuni sul lavoro; gli artt. 216 e seguenti della legge fallimentare puniscono la sottrazione, da parte dell'imprenditore, delle garanzie patrimoniali che le procedure concorsuali mirano a garantire; gli illeciti in materia di scarico o emissione nell'aria o nelle acque puniscono la violazione delle rispettive regole di condotta fissate dal D. Lgs. n. 152/2006; i reati previsti dagli artt. 12 e 13 della legge n. 40/2004 e dall'art. 22 della legge n.91/1999 comminano una pena a chi violi le disposizioni relative alla fecondazione medicalmente assistita o quelle sui trapianti etc.

8 L'importanza delle fonti di autoregolazione è oggi ribadita dal "considerando" n. 44 della Direttiva c.d. NIS (si veda infra), secondo cui *«è opportuno promuovere e sviluppare attraverso adeguati obblighi regolamentari e pratiche industriali volontarie una cultura della gestione del rischio, che comprende la valutazione del rischio e l'attuazione di misure di sicurezza commisurate al rischio corso».*

9 Dizionario di Italiano, Garzanti, voce *Compliance*, 2010, p. 728

quindi su disposizioni di scaturigine endosocietaria – o più in generale, privata – le quali, indirettamente, incidono sulla portata di norme vincolanti di emanazione pubblica (DE BENEDETTO, 2005)[10]. L'autoregolazione colma gli spazi lasciatigli dalla regolazione e supplisce, talvolta, alle carenze di essa (BOSI, 2009): nessun processo di azione sociale potrebbe essere completamente autonomo, né interamente eteronomo (MAGGI, 2003). Ciò risulta tanto più vero nelle organizzazioni complesse nelle quali, da una parte, l'azione giuridica risulta vincolata dal sistema di regole istituzionali che la governano; dall'altra il ruolo di chi decide e l'apparato gerarchico di riferimento possono dar luogo ad un sistema di autoregolazione (ZANIER, 2012).

L'incidenza delle regole di condotta "autodisciplinari" sulla latitudine della responsabilità penale sembrerebbe scontrarsi con un limite insuperabile: il rispetto del principio di legalità, in base al quale gli elementi costitutivi della fattispecie di reato debbono essere dettati da una norma primaria di legge (PALAZZO,1999; MANTOVANI, 2002). Invero, tale principio non esclude che le fonti di autoregolazione siano prese in considerazione per il tramite di elementi normativi "elastici" della fattispecie (MARANI, 2014; RISICATO, 2004)[11], o di clausole generali (CASTRONUOVO, 2012), e che esse conformino, in tal modo, la portata della disposizione incriminatrice.

Venendo ora al tema che ci occupa, si possono richiamare alcune ipotesi in cui l'autoregolazione nel settore della sicurezza informatica incide sulla responsabilità penale dei destinatari delle regole di condotta.

Considerando la *cybersecurity* dalla prospettiva della protezione delle confidenzialità e della disponibilità di informazioni possono addursi due esempi:

10 Quella che, comunemente, viene definita "regolazione". La nozione di regolazione cui facciamo riferimento è quella delineata dall'OCSE come «*the diverse set of instruments by wich governments set requirements in enterprises and citizens».* Cfr. OCSE*, Report on Regulatory Reform*, Parigi, 1997, p. 6.
Il documento è disponibile sul sito internet istituzionale al seguente collegamento: *https://www.oecd.org/gov/regulatory-policy/2391768.pdf*

11 Il primo autore definisce "elastici" gli elementi che esprimono concetti che ammettono un margine di possibili soluzioni opposte, dipendenti dall'apprezzamento del giudice, margine che, però, non priva la norma della sua sufficiente determinatezza. La seconda, invece, definisce tali quelli la cui interpretazione è contraddistinta da una duplice linea di confine, una zona grigia all'interno della quale confluisce una gamma di accezioni affidate, per la loro concreta definizione, alla sensibilità del singolo interprete.

l'accesso abusivo a sistema informatico (art. 615-*ter* c.p.) per quel che riguarda la *compliance* nel settore privato; l'agevolazione colposa nella rivelazione di segreti d'ufficio (art. 326, comma 2, c.p.) con riferimento al contesto pubblico.

Quanto alla prima, la fattispecie punisce *«chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo».*

Si pensi ora al caso in cui una società adotti, a tutela del *know-how*, un regolamento interno sull'utilizzo di una piattaforma informatica contenente informazioni di carattere commerciale sui propri prodotti. Detto regolamento prevede che i dipendenti possano accedervi soltanto per finalità strettamente connesse al servizio, qualora autorizzati da un dirigente. La violazione delle predette disposizioni potrebbe comportare, di là dell'apertura del procedimento disciplinare, una qualche conseguenza sul piano penale?

La giurisprudenza maggioritaria ritiene il reato integrato anche dalla condotta del soggetto che, pur munito di regolare *password* – e dunque legittimato ad accedere al sistema – si introduca o si mantenga in esso per ragioni o finalità diverse da quelle giustificatrici dell'accesso e ciò in violazione delle specifiche disposizioni dettate dal titolare del sistema (FERRETTI, 2015)[12]. La norma, in realtà, aveva dato luogo ad un contrasto interpretativo, risolto dalle Sezioni Unite (PECORELLA, 2012; per gli orientamenti precedenti CUOMO, IZZI, 2002)[13] nel senso che l'accesso e il trattenimento nel sistema informatico è

12 Cfr. Cass. Pen., Sez. V, 11 marzo 2015 n. 32666, la quale ha affermato che *«nel caso di soggetto munito di regolare password, è necessario accertare il superamento, su un piano oggettivo, dei limiti e, pertanto, la violazione delle prescrizioni relative all'accesso ed al trattenimento nel sistema informatico, contenute in disposizioni organizzative impartite dal titolare dello stesso, indipendentemente dalle finalità soggettivamente perseguite».*

13 Cass. Pen., Sez. Un., 27 ottobre 2011 n. 4694 in *Cass. Pen*. 2012, 11, p. 3681ss. Il Consesso era stato chiamato a pronunciarsi *«se integri la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto abilitato ma per scopi o finalità estranei a quelli peri quali la facoltà di accesso gli è stata attribuita».* In seno alla Suprema Corte vi era infatti un orientamento che escludeva, in ogni caso, che il reato di cui all'art. 615-*ter* c.p. fosse integrato dalla condotta del soggetto il quale, avendo titolo per accedere al sistema, se ne avvalga per finalità estranee a quelle di ufficio (cfr. *ex multis* Cass. Pen. Sez. V, 20 dicembre 2007 n. 2534, in *Riv. Pen.,* 2008, 6, p. 655 ss). Un secondo orientamento riteneva invece rilevante, ai fini dell'integrazione del reato *de quo*, anche la condotta del soggetto che, pure

abusivo allorquando l'agente violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema. La nozione di "prescrizioni" viene specificata dalla Corte facendo riferimento alla violazione delle prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro[14].

Ecco dunque che le fonti di autoregolazione circa l'utilizzo del sistema informatico – e quelle che, più in generale disciplinano l'accesso ad informazioni riservate – incidono sulla portata estensiva del precetto penale. Così, nel caso pocanzi esemplificato, la violazione delle procedure interne dettate dal regolamento concorrerà a qualificare l'accesso come "abusivo" in senso penalistico.

Il secondo esempio riguarda la sicurezza sotto il profilo della tutela della confidenzialità delle informazioni apprese dai pubblici agenti. L'adozione di modelli di *cybersecurity* incide sull'accertamento della colpa nella condotta di agevolazione prevista dal secondo comma dell'art. 326 c.p.

Si pensi al caso in cui il dirigente di un ente pubblico, dopo aver salvato sul *pc* alcuni documenti segreti che riguardano il proprio ufficio, disattivi (o ometta di attivare) il *firewall*, non esegua gli aggiornamenti dell'*antivirus,* oppure ometta di proteggere l'accesso con chiavi segrete. *Quid iuris* se il computer è colpito da un attacco informatico o diviene oggetto di un accesso abusivo con il quale terzi si impossessano dell'informazione segreta?

Il codice penale punisce il pubblico agente che *«violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rivela notizie*

essendo abilitato ad accedere al sistema informatico o telematico, vi si introduca con la *password* di servizio per raccogliere dati protetti per finalità estranee alle ragioni di istituto ed agli scopi sottostanti alla protezione dell'archivio informatico, utilizzando sostanzialmente il sistema per finalità diverse da quelle consentite (cfr. *ex plurimis* Cass. Pen. 07 novembre 2000 n. 12732 in *Cass. Pen*. 2002, p. 1015).

14 Il tema è ancora "caldissimo" in giurisprudenza. Lo scorso 18 maggio 2017 le Sezioni Unite sono state chiamate a pronunciarsi "se integri il delitto previsto dall'art. 615-*ter*, secondo comma, n. 1, cod. pen. la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita". Al quesito è stata data risposta affermativa, su parere conforme del Procuratore Generale, con sentenza n. 41210 depositata lo scorso 08 settembre 2017.

di ufficio, le quali debbano rimanere segrete, o ne agevola in qualsiasi modo la conoscenza» (art. 326, comma 1), ciò anche *«se l'agevolazione è soltanto colposa»* (art. 326, comma 2). È opinione diffusa che la condotta di agevolazione sia integrata anche dal semplice lasciare incustodito (ANTOLISEI, 2008; ROMANO, 2013; FIANDACA, MUSCO, 2012) il documento contenente l'informazione segreta; nel caso di documento in formato digitale l'omessa custodia avrà riguardo alla mancata adozione di misure di protezione di carattere informatico.

La *governance* del cyber rischio nel contesto pubblico è disciplinata da disposizioni di particolare rilevanza (SEVERINO, 2017). Sulla Gazzetta Ufficiale sono state di recente[15] pubblicate le *"Misure minime di sicurezza ICT per le Pubbliche Amministrazioni"*[16] le quali costituiscono parte integrante delle Linee Guida per la sicurezza ICT. Il documento riporta una serie di tabelle[17] sulle disposizioni tecniche e i protocolli informatici di base, lasciando alla discrezionalità di ciascuna Amministrazione l'attività di valutazione del rischio e la concreta attuazione di misure ulteriori di tutela[18].

Tale fonte di (auto-)regolazione pubblica del *cyber risk* istituisce una sorta di "paradigma cautelare" di base, rimettendo alle singole amministrazioni la concreta attuazione di misure più incisive. Il riconoscimento di uno *standard* a livello internazionale accredita l'idea che le misure minime di sicurezza trovino

15 *Gazzetta Ufficiale della Repubblica Italiana,* Serie Generale, 04 aprile 2017, n. 79 p. 50 ss.

16 Il documento, varato in attuazione della Direttiva del Presidente del Consiglio dei Ministri del 1 agosto 2015, costituisce *«un'anticipazione urgente della regolamentazione completa in corso di emanazione, al fine di fornire alle pubbliche amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento»*. La Direttiva del 2015 aveva sollecitato tutte le Amministrazioni a dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di *standard* minimi di prevenzione e reazione ad eventi cibernetici. A fine di agevolare tale processo l'Agenzia per l'Italia Digitale
è stata impegnata a rendere prontamente disponibili indicatori degli *standard* di riferimento.

17 Si prevedono diverse "classi" di misure, in base agli indicatori forniti dall'Agenzia per l'Italia Digitale (c.d. *AgID Basic Security Controls*, ABSC). Questi ultimi, a loro volta, si riportano all'insieme di controlli (noto come SANS 20), pubblicati dal *Center for Internet Security*, con la denominazione *Critical Security Controls for Effective Cyber Defense* nella versione 6.0 di ottobre 2015

18 Il documento prevede, infatti, che ciascuna amministrazione *"dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi"* (p. 54).

ragione in una valutazione di prevedibilità ed evitabilità dell'evento – sia essa la perdita o la diffusone dei dati – secondo la comune esperienza degli esperti del settore.

Nel caso esemplificato, il dirigente che abbia agevolato la presa di conoscenza altrui del documento informatico omettendo di adottare le doverose cautele sarà rimproverabile per colpa specifica, consistita nel non essersi adeguato alle disposizioni appartenenti alla prima classe delle misure minime[19]. Il modello di regolazione pubblica della sicurezza ICT è quindi rilevante per accertamento della responsabilità del pubblico agente, potendo rientrare tra le "discipline" richiamate dall'art. 43 c.p. (FORTI, 1990; BONAFEDE, 2005; CASTRONUOVO, 2009).

I casi che abbiamo esaminato mettono in evidenza che la *compliance* in materia di *cybersecurity,* è in grado di incidere sulla configurabilità, in termini oggettivi e soggettivi, dell'illecito penale, e che ciò è vero tanto nel settore privato quanto in relazione all'autoregolazione nell'ambito delle P.A.

In conclusione, l'assenza di fattispecie incriminatrici *ad hoc* e di una organica disciplina di settore non sembra essere d'ostacolo alla rilevanza "esterna" della *cybersecurity* nel riempire di contenuto gli elementi normativi di alcune fattispecie penali.

4. La Direttiva c.d. NIS e le prospettive di tutela penale. Soltanto in tempi recenti la *cybersecurity* – abbandonato l'alveo della *compliance* societaria – si è affermata a livello legislativo.

Più precisamente, guardando all'ordinamento eurounitario, l'adozione della direttiva 2016/1148/UE *(misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione)* ha segnato un passo decisivo verso l'armonizzazione delle legislazioni degli Stati membri nel settore della sicurezza delle reti e dei sistemi di informazione.

19 Che prevedono, tra gli altri, l'obbligo di dotare il sistema informatico di chiavi di accesso e di protezione dall'attacco di virus in base alle disposizioni del SANS 20.

Nel disciplinare gli obblighi cui saranno tenuti gli Stati membri, il legislatore europeo valorizza la centralità della *governance*[20] del rischio cibernetico. Infatti, per conseguire e mantenere un livello elevato di sicurezza della rete e dei sistemi informativi è anzitutto opportuno che *«ogni Stato membro disponga di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi che definisca gli obiettivi strategici e gli interventi strategici concreti da attuare»*[21]*,* e che la pianificazione degli obiettivi sia resa effettiva mediante l'istituzione di un'Autorità nazionale competente responsabile di soddisfare i compiti connessi alla sicurezza delle reti e dei sistemi informativi (artt. 7 e 8)[22]. Essendo la sicurezza delle reti e delle informazioni un'esigenza comune al settore pubblico e a quello privato, vengono incoraggiante forme di cooperazione spontanea, anche grazie al coordinamento dell'ENISA e delle Autorità nazionali (artt. 10 e 11).

La responsabilità di garantire la sicurezza delle reti e dei sistemi informativi incombe in larga misura sugli operatori di servizi essenziali e sui fornitori di servizi digitali che sono i principali destinatari degli obblighi di prevenzione e notifica degli incidenti. Con riferimento all'attività svolta da queste categorie di soggetti, il legislatore dell'Unione riconosce l'importanza della prevenzione del *cyber-risk* (SEVERINO, 2017)*,* attribuendo rilievo all'adozione di regolamenti interni e prassi industriali: una cultura della gestione del rischio, che comprende la valutazione del rischio e l'attuazione di misure di sicurezza commisurate al rischio (SEVERINO, 2017)[23]. L'art. 14 dispone infatti che gli Stati debbano provvedere affinché gli operatori di servizi essenziali adottino «*misure tecniche e organizzative adeguate e proporzionate alla*

20 L'art. 7, par. 1, lett. b) prevede che il piano strategico nazionale debba predisporre *«un quadro di governance per conseguire gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti»*.

21 Così il "considerando" n. 29

22 Il legislatore europeo vuole che ciascuno Stato si doti delle capacità tecniche e organizzative necessarie a prevenire, individuare, rispondere e attenuare i rischi e gli incidenti a carico delle reti e dei sistemi informativi. Pertanto gli Stati dovranno anche assicurare la disponibilità di squadre di pronto intervento informatico («CERT»), in modo da garantire l'esistenza di capacità effettive e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello di Unione (Cfr. "considerando" n. 35).

23 In tal senso si veda il "considerando" n. 44

gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni» (par. 1) e *«misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi»* (par. 2). Non diversamente, il successivo art. 16, par. 1, prevede che i fornitori di servizi digitali *«identifichino e adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano».*[24]

Quanto alle implicazioni in termini di responsabilità individuale e collettiva del *framework* delineato dalla Direttiva *NIS*, è bene evidenziare che all'orizzonte si intravedono scenari di indubbio interesse per il penalista. Ciascuno Stato membro sarà tenuto a comminare sanzioni effettive, proporzionate e dissuasive in caso di violazione delle disposizioni nazionali di attuazione[25].

Pur non intervenendo direttamente in materia penale ai sensi dell'art. 83 TFUE[26] – e dunque lasciando alla discrezionalità degli Stati membri l'individuazione della natura dell'illecito – la Direttiva apre le porte alla eventuale introduzione di fattispecie sanzionatorie di penalistico rilievo, indipendentemente dal *nomen iuris* che il legislatore intenderà attribuir loro. Se si guarda alla coerenza sistematica con la disciplina in materia di protezione dei dati personali – specie per quel che riguarda l'adozione di misure minime di sicurezza, l'osservanza dello *standard* previsto dal Regolamento[27], e la

24 La disposizione precisa che, tenuto conto delle conoscenze più aggiornate in materia, le misure "prevenzionistiche" debbano assicurare un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente, tenendo conto dei seguenti elementi: a) la sicurezza dei sistemi e degli impianti; b) trattamento degli incidenti; c) gestione della continuità operativa; d) monitoraggio, audit e test; e) conformità con le norme internazionali.

25 L'art. 21 della Direttiva dispone che *«gli Stati membri stabiliscono le norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva e adottano tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste sono effettive, proporzionate e dissuasive».*

26 La *cybersecurity* è materia fortemente connessa alla prevenzione della criminalità informatica. La violazione delle disposizioni sulla sicurezza delle reti e delle informazioni, in linea di principio, ben potrebbe rientrare nelle sfere di criminalità per le quali l'art. 83, par. 1, del Trattato sul Funzionamento dell'Unione Europea ammette la fissazione di *minimum rules*. Una competenza in materia penale nel settore *de quo* potrebbe comunque ricondursi alla *annex compentence* di cui al par. 2 del medesimo articolo.

27 L'omissione di misure di sicurezza, l'inottemperanza ai provvedimenti dell'Autorità Garante e violazione dei diritti degli interessati soggiacciono alle sanzioni previste dall'art. 83, par. 5:

violazione degli obblighi di notifica dei *data breach*[28] – è dato credere che agli operatori dei servizi essenziali e ai fornitori di servizi digitali saranno imposte sanzioni estremamente onerose in caso di mancata attuazione delle misure tecniche. Dalla prospettiva della tutela dei dati personali *digital privacy* e *cybersecurity* costituiscono un sistema integrato di protezione, caratterizzato da reciproche interferenze e punti di contatto[29]: ne consegue che le fattispecie di illecito di futura introduzione *ex* art. 21 cit., dovrebbero prevedere sanzioni particolarmente incisive a carico dei soggetti destinatari degli obblighi di protezione e prevenzione.

Il tema della gravosità delle sanzioni richiama alla mente il concetto di *matière pénal* plasmato dalla giurisprudenza della Corte di Strasburgo a partire dalla storica sentenza *Engel* fino agli approdi più recenti (VIGANÒ, 2017; SCAROINA 2015; FLICK, NAPOLEONI, 2015; TRIPODI, 2014)[30]. Verrebbe quindi a

sanzione amministrativa fino a 20 000 000 EUR e, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente.
Il Trattamento non conforme alle disposizioni del Regolamento e violazione dei diritti degli interessati sono punite dall'art. 83, par. 4, con sanzioni amministrative fino a 10 000 000 EUR, e, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente.

28 È definito *data breach* «*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati». (*art. 7 Regolamento 2016/679/UE*);* la violazione dei dati personali fa sorgere l'obbligo di notifica all'Autorità di controllo (art. 33), la cui inottemperanza è sanzionata dall'art. 83, par. 4 del Regolamento Generale.

29 Non a caso l'art. 8, par. 6, della Direttiva *NIS* dispone che *«ove opportuno e conformemente al diritto nazionale, le autorità competenti e il punto di contatto unico consultano le autorità di contrasto e le autorità per la protezione dei dati nazionali competenti e collaborano con esse».*

30 La questione, ancora oggi al centro di un copioso dibattito scientifico, concerne i limiti esterni della c.d. materia penale, cioè quando sia possibile attribuire carattere penale ad una sanzione, ai fini dell'applicazione dell'art. 4 del Protocollo 7 della Convenzione Europea dei diritti dell'uomo e dell'art. 6 della Convenzione medesima. Sul punto la Corte di Giustizia di Strasburgo fa costante riferimento ai c.d. criteri elaborati con la sentenza *Engel c. Paesi Bassi* del 8 giugno 1976 e progressivamente affinati.
In estrema sintesi, la Corte ritiene che, al fine di verificare se un procedimento abbia ad oggetto "accuse in materia penale", si dovrebbero considerare tre diversi fattori.
Anzitutto, la qualificazione attribuita dal sistema giuridico nazionale all'illecito contestato; a tale indicazione va però riconosciuto un valore soltanto formale e relativo poiché la Corte deve supervisionare sulla correttezza di tale qualificazione alla luce degli altri fattori indicativi del carattere "penale" dell'accusa.
In seconda istanza, infatti, va considerata la natura sostanziale dell'illecito commesso vale a dire se si è di fronte ad una condotta in violazione di una norma che protegge il funzionamento di una determinata formazione sociale o se è invece preposta alla tutela *erga omnes* di beni giuridici della collettività, anche alla luce del denominatore comune delle rispettive legislazioni dei diversi Stati contraenti.

delinearsi un diritto sanzionatorio di natura marcatamente penalistica, quand'anche il legislatore lo configurasse attraverso illeciti formalmente amministrativi. La Corte EDU è infatti ferma nel ritenere che il carattere penale di un procedimento è subordinato al grado di gravità della sanzione di cui è *a priori* passibile la persona interessata, a prescindere dalla gravità della sanzione in concreto irrogata[31].

Da altro punto di vista, l'imposizione di obblighi di *compliance*[32] nel settore della sicurezza informatica – non diversamente da quanto si è detto a proposito delle fonti di autoregolazione – riverbera i propri effetti sull'estensione di concetti generali del diritto penale, quali ad esempio la colpa specifica, la posizione di garanzia, la prevenibilità dell'evento dannoso, l'agevolazione della condotta illecita altrui. In tal senso, la regolazione della *cybersecurity* è in grado di esercitare un'efficacia indiretta sul raggio d'azione del diritto penale.

Per concludere, sembra che l'intero sistema di *cybersecurity* ruoti attorno a tre fattori: l'importanza delle fonti autoregolamentari, l'individuazione delle fonti di rischio, e l'adozione di misure tecniche e organizzative adeguate a far fronte al rischio individuato. Tali elementi caratterizzanti richiamano alla mente i

---

Infine si deve considerare il grado di severità della pena comminata al responsabile, poiché in una società di diritto appartengono alla sfera "penale" tutte quelle sanzioni che incidono in modo significativo sull'esercizio di diritti e libertà fondamentali.
La CEDU ritiene, dunque, che si debba considerare di natura penale la sanzione che sia qualificata tale dalla norma che la prevede e che, in mancanza, si debba tener conto della natura della violazione o della natura, scopo e gravità della sanzione. In argomento, *ex plurimis* CEDU sent. causa C-199/92 del 1999 *Huls c. Commissione*; sentenza 21 febbraio 1984 *Ozturk c. Germania*, serie A n. 73, par.53; più di recente, in materia di illeciti di *market abuse*, la celebre sentenza *Grande Stevens c. Italia* del 4 marzo 2014 (ric. 2010 n. 18640, 18647, 18663, 18668 e 18698) in *Dir. Pen. Cont*., 9 marzo 2014; da ultimo, in materia di illeciti tributari la sentenza 18 maggio 2017*, Jóhannesson e a. c. Islanda*, (ric. n. 22007/11), in *Dir. Pen. Cont*., 22 maggio 2017.
31 In questo senso la sentenza *Grande Stevens c. Italia, cit*., § 98 nel richiamare la precedente *Engel c. Paesi Bassi, cit.*, § 82. Ancor più di recente, con riferimento alla disciplina sanzionatoria tributaria, si vedano le conclusioni rassegnate lo scorso 12 settembre dall'Avvocato Generale della Corte di Giustizia nella Causa C-524/15 *Menci e altri,* disponibili, con traduzione in lingua italiana, sul sito internet istituzionale della Corte di Giustizia nella sezione dedicata alla ricerca sulle pronunce:
http://curia.europa.eu/juris/recherche.jsf?language=it
32 Intesi quale necessità, per gli operatori qualificati, di adottare *«misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi»* e *«misure adeguate per prevenire e minimizzare l'impatto di incidenti»* (art. 14 della Direttiva NIS).

principi giuseconomici del *risk management* e *assessment*, spesso richiamati con riferimento al sistema di responsabilità degli enti *ex* D. Lgs. 231/2001.

De iure condendo sarebbe opportuno che il sistema evolvesse verso una maggiore responsabilizzazione della sfera collettiva, e che l'apparato sanzionatorio – sia esso penale o amministrativo – fosse modellato attorno alla persona giuridica, anziché quella fisica. Del resto, le figure soggettive gravate dagli obblighi di sicurezza (operatori dei servizi essenziali, fornitori di servizi digitali) si identificano in realtà societarie estremamente articolate e complesse, il che renderebbe inopportuno l'introduzione di forme di responsabilità (soltanto) individuale.

5. Conclusioni. Il panorama normativo attuale non consente di affermare l'esistenza di un diritto penale della sicurezza informatica e della protezione cibernetica. Si tratta di una materia che, fino ad oggi, si è evoluta in seno alle organizzazioni complesse attraverso le fonti di autoregolazione.

Tuttavia, il ruolo della *compliance* nel governo del cyber-rischio si palesa di fondamentale importanza e, talvolta, incide sul *range* d'azione del diritto penale: può infatti accadere che il precetto di alcune fattispecie di reato si presti ad essere riempito di contenuto attraverso il richiamo implicito alle disposizioni autoregolamentari o che l'estensione di alcune clausole generali o elastiche vada parametrato a quest'ultime.

Con la Direttiva NIS il legislatore europeo ha riaffermato, a livello positivo, la centralità dell'adozione di piani, strategie e misure di *governance* del rischio cyber non solo a livello di politica nazionale, ma soprattutto per gli operatori dei servizi essenziali e i fornitori di servizi digitali. In prospettiva futura, quindi, ci si attende che il diritto sanzionatorio evolva nel senso di una radicale responsabilizzazione delle persone giuridiche per l'omessa adozione delle misure tecniche e organizzative idonee a prevenire e minimizzare l'impatto delle minacce del cyberspazio.

Il futuro, dunque, vede la *compliance* come fattore di garanzia della sicurezza dei dati e della protezione delle informazioni. Che sia proprio questa

– per tornare alla metafora d'apertura – la *longa manus* dello Stato, l'arma mitologica "capace di offendere e guarire", pur di preservare la libertà di *internet*?

Riferimenti bibliografici

ANTOLISEI F., *Manuale di diritto penale. Parte speciale*. Vol.II, Milano, 2008, p. 395
BONAFEDE M, *L'accertamento della colpa specifica,* Padova, 2005, p. 62
BOSI G., *Autoregolazione societaria*, Milano, 2009, p. 109 ss.
CARCATERRA G., *Presupposti e strumenti della scienza giuridica,* Torino, 2011, p. 3
CASTRONUOVO D., *Clausole generali e diritto penale*, in *Dir. Pen. Cont*., 14 novembre 2012, p. 3 ss
CASTRONUOVO D., *La colpa penale*, Milano, 2009 p. 130 ss
CUOMO L., IZZI B., *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*), in *Cass. Pen*. 2002, p. 1015
DE BENEDETTO M., *L'organizzazione della funzione di regolazione*, in *Studi parlamentari e di politica costituzionale*, 2005, fasc. 149-150, p. 73 ss
FERRETTI A., *Irrilevante per la configurazione del reato di accesso abusivo in un sistema informatico la finalità che ha motivato l'ingresso*, in *Diritto & Giustizia*, fasc. 30, 2015, p. 81 ss
FIANDACA G. MUSCO E., *Diritto Penale. Parte speciale*., vol. I, Milano, 2012, p. 264
FLICK G.M., NAPOLEONI V., *A un anno di distanza dall'"Affaire Grande Stevens": dal "bis in idem" all'"e pluribus unum"?* in *Rivista AIC*, 2015, fasc. 3, pp. 34;
FORTI G., *Colpa ed evento nel diritto penale*, Milano, 1990 p. 309
MAGGI B., *De l'agir organisationnel: un point de vue sur le travail, le bien-être, l'apprentissage*, Toulouse, 2003, p. 25
MANTOVANI F., *Principi di diritto penale*, Padova, 2002 p. 3 ss.
MARANI S., *Principio di determinatezza e norma integratrice del precetto penale*, Firenze, 2014 p. 32
PALAZZO F., *Introduzione ai principi del diritto penale*, Torino, 1999, p. 199 ss;
PECORELLA C., *L'attesa pronuncia delle Sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo,* in *Cass. Pen*. 2012, 11, p. 3681 ss.
PICOTTI L., *Diritti fondamentali nell'uso e nell'abuso dei social network. Aspetti penali.*, in *Giur. mer*., 2012, 12, p. 2523
RISICATO L., *Gli elementi normativi della fattispecie penale*, Milano, 2004, p. 197
RODOTÀ S., *Una Costituzione per Internet*, in *Pol. dir*. 2010, 3, p. 339
ROMANO M., *Commentario sistematico al codice penale. I delitti contro la pubblica amministrazione. I delitti dei pubblici ufficiali*, Milano, 2013, p. 307;
SCAROINA E., *Costi e benefici del dialogo tra corti in materia penale. La giurisprudenza nazionale in cammino dopo la sentenza Grande Stevens tra disorientamento e riscoperta dei diritti fondamentali*, in *Cass. Pen*., 2015, fasc. 7-8, pp. 2910-2943.
SEVERINO P., *Le frontiere della sicurezza informatica e prevenzione del cybercrime*, in *Luiss Open,* 8 settembre 2017 p. 8 ss.;
TRIPODI A. F., *Uno più uno (a Strasburgo) fa due. L'Italia condannata per violazione del ne bis in idem in tema di manipolazione del mercato*) in *Dir. Pen. Cont*., 9 marzo 2014
VIGANÒ F., *Una nuova sentenza di Strasburgo su ne bis in idem e reati tributari*, in *Dir. Pen. Cont*., 22 maggio 2017
ZANIER M.L., *L'accusa penale in prospettiva socio-giuridica*, Milano 2012 p. 28
ZICCARDI G., *Cyber Law in Italy*, 2011, NL, p. 15 ss

Una spinta verso la trasformazione tecnologica delle imprese: l'iperammortamento come strumento di politica fiscale per l'innovazione

di **ALESSANDRO LIOTTA**

Abstract

This paper addresses the so-called "iperammortamento" of the new assets, aimed at the technological transformation and evolution of the business enterprise, in an "**Industry 4.0**" perspective. It is a fiscal policy instrument introduced by Law December 11th, 2016, n. 232, (the 2017 Italian Budget Law), that allows the increase of the amortization rates and of the leasing fees up to 150% of the purchase cost. The aim of this paper is to analyse the tax benefit at issue, among the tax instruments introduced in the last years to boost R&D activities and the process of technological innovation of the Italian business enterprises. Also, it might be useful to compare this tool with the "superammortamento", as introduced by the 2016 Italian Budget Law.
Finally, the Circular n. 4/E, issued by the Italian Tax Administration on March 30th, 2017, plays a significant role, as it makes it clear how the "superammortamento" can be applied and faces the issues arising from the "iperammortamento" for the first time.

1. Introduzione. L'industria 4.0 e lo sviluppo tecnologico delle imprese. L'espressione "Industria 4.0" sta ad indicare il processo evolutivo che il settore industriale sta vivendo nell'epoca attuale, assimilabile ad una vera e propria rivoluzione industriale. Il progresso tecnologico cui si è assistito negli ultimi anni ha avuto un notevole impatto non solo nella vita quotidiana ma anche, e soprattutto, nel settore industriale, dove considerevole è stata la sua incidenza. Secondo il "Piano Nazionale Industria 4.0" del Ministero dello Sviluppo Economico, tale rivoluzione tecnologica dovrebbe rendere più efficace ed efficiente la produzione industriale nel nostro Paese, che ne beneficerà sotto diversi profili[1].

1Secondo il Ministero dello Sviluppo Economico i benefici derivanti dal suddetto Piano Nazionale sarebbero i seguenti: *maggiore flessibilità* attraverso la produzione di piccoli lotti ai costi della grande scala; *maggiore velocità* dal prototipo alla produzione in serie attraverso tecnologie innovative; *maggiore produttività* attraverso minori tempi di set-up, riduzione errori e

A ben vedere, l'Italia non è il primo Paese ad aver elaborato un programma mirato ad un miglioramento della produzione industriale globale mediante il progresso tecnologico[2]. Per colmare questo distacco con altri Paesi industrializzati, il Ministero dello Sviluppo ha diramato talune direttrici strategiche di intervento, nel quadro del Piano Nazionale Industria 4.0 2017-2020[3]. Evidentemente, in un periodo di difficoltà economica per le imprese, siffatto sviluppo tecnologico non può che essere spinto e incentivato dallo Stato, cui si richiede un notevole sforzo, anche creativo, per creare gli strumenti necessari affinché le imprese possano attrezzarsi adeguatamente ed in linea con i progressi della tecnica.

Ed invero lo strumento più efficace che lo Stato può adottare e che si presta di più alle esigenze delle imprese è rappresentato dalle agevolazioni fiscali. L'intervento dello Stato, dunque, si sostanzia in buona parte anche in una previsione di minor gettito a breve termine, per consentire alle imprese che si sono dotate di più moderni ed efficienti sistemi produttivi, che hanno investito in attività di ricerca e sviluppo, che hanno acquistato beni immateriali funzionali all'esercizio dell'attività d'impresa o che hanno realizzato tali *intangibles*, di

---

fermi macchina; *migliore qualità*, e minori scarti mediante sensori che monitorano la produzione in tempo reale; *maggiore competitività* del prodotto grazie a maggiori funzionalità derivanti dall'Internet delle cose.

2 Si pensi al programma "*Manifacturing* USA", che comporta la realizzazione di network di istituti e di laboratori di eccellenza, per la diffusione tecnologica e delle competenze, e che implica un supporto pubblico a progetti di ricerca, anche universitari; o anche al programma "*Industrie du Futur*" francese, ossia il piano di reindustrializzazione e di investimento in tecnologie Industria 4.0 guidato centralmente dal Governo, e che si basa su una serie di misure pubbliche, quali incentivi fiscali per investimenti privati, prestiti agevolati per piccole e medie imprese, credito d'imposta per attività di ricerca e finanziamento di progetti basati sulla c.d. "industria del futuro"; o ancora al piano d'azione federale tedesco denominato "Industrie 4.0", che coinvolge anche grandi soggetti industriali e tecnologici e che prevede un finanziamento pubblico alle progettualità aziendale e ai centri di ricerca applicata, nonché agevolazioni fiscali per investimenti in start-up tecnologiche.

3 Tali direttrici vengono distinte in *direttrici chiave* (incentivare gli investimenti privati su tecnologie e beni Industria 4.0; aumentare la spesa privata in Ricerca, Sviluppo e Innovazione; rafforzare la finanza a supporto di Industria 4.0 e start-up; diffondere la cultura Industria 4.0 attraverso Scuola Digitale e Alternanza Scuola Lavoro; sviluppare le competenze Industria 4-0 attraverso percorsi universitari e istituti tecnici superiori dedicati; finanziare la ricerca Industria 4.0 potenziando i cluster e i dottorati) e *direttrici di accompagnamento* (assicurare adeguate infrastrutture di rete con il Piano Banda Ultra Larga; collaborare alla definizione di standard e criteri di interoperabilità nell'internet delle cose; garantire gli investimenti privati; supportare i grandi investimenti innovativi; rafforzare e innovare il presidio di mercati internazionali; supportare lo scambio salario-produttività attraverso la contrattazione decentrata aziendale).

godere di condizioni favorevoli nel mercato e di incrementare e migliorare la propria produzione. Scopo primario delle misure contenuto nel Piano Nazionale Industria 4.0 è lo sviluppo tecnologico di tutte le imprese, pubbliche e private, e il coinvolgimento della società a più livelli, dagli istituti di ricerca e le università ai c.d. *big players* e ai grossi poli industriali, in un processo che possa permettere all'intera società di beneficiare delle innovazioni tecnologiche tipiche dell'era digitale.

2. Alcune misure di sostegno all'innovazione. Una panoramic generale. Orbene, come si è in precedenza avuto modo di accennare, il nostro ordinamento giuridico si è dotato negli ultimi anni di una pluralità di strumenti, alcuni tra loro cumulabili, che possono consentire alle imprese di ottenere significativi risultati nel contesto dell'Industria 4.0.

Appare doveroso, pertanto, occuparsi brevemente e senza pretese di esaustività, di alcuni strumenti fiscali che il Legislatore ha introdotto con il precipuo obiettivo di rilanciare l'attività di ricerca e sviluppo e l'innovazione[4] tecnologica.

Si pensi, ad esempio, alla c.d. *Legge Sabatini-ter*, ossia il Decreto Legge 21 giugno 2013, n. 69, come convertito e modificato dalla Legge 9 agosto 2013, n. 98, ed implementato dal Decreto Ministeriale 27 novembre 2013, n. 72982, che prevede «l'erogazione di un contributo da parte del Ministero dello Sviluppo Economico a parziale copertura degli interessi relativi a finanziamenti stipulati per l'acquisto o acquisizione in leasing di beni strumentali nuovi» (R. FRISCOLANTI – B. PAGAMICI 2017). Tale agevolazione fiscale, che, secondo la normativa originaria, si prevedeva dovesse scadere il 31 dicembre 2016, è stata estesa temporalmente ed oggettivamente dall'art. 1, commi 52-57, Legge 11 dicembre 2016, n. 232 (*Legge di Bilancio 2017*). In particolare, l'ultima legge di bilancio non solo ha permesso di prorogare l'agevolazione fiscale in oggetto

4 Tratto qualificante della ricerca di impresa sembra potersi individuare nella innovazione, e cioè nella individuazione di elementi innovativi ed aggiuntivi rispetto alla piattaforma di conoscenze acquisite nel settore di mercato in cui opera l'impresa. In merito al concetto di innovazione e di attività di ricerca.

fino al 31 dicembre 2018, ma ha anche ampliato il suo ambito di operatività, coinvolgendo anche gli investimenti in tecnologie digitali e in sistemi di tracciamento e pesatura dei rifiuti, per i quali il contributo dello Stato è pari al 3,575% annuo[5] e gli investimenti ordinari (investimenti diversi dai precedenti, per i quali il contributo è pari al 2,75% annuo).

In altri termini l'agevolazione introdotta dalla Legge Sabatini-*ter* prevede, in estrema sintesi, la concessione di un contributo alle PMI e copertura parziale degli interessi su finanziamenti bancari quinquennali di macchinari, impianti e attrezzature. Con la Legge di Stabilità 2017 si inserisce nel tessuto normativo la possibilità di un contributo maggiorato nel caso di investimenti in tecnologie digitali, compresi gli investimenti in *Big Data*, *cloud computing*, banda ultra-larga, *cybersecurity*[6], robotica avanzata e meccatronica, realtà aumentata, manifattura 4D, *Radio frequency identification*, integrati in sistemi di tracciamento e pesatura dei rifiuti.

In precedenza, con il Decreto Legge 18 ottobre 2012, n. 179 (artt. 25-32), come convertito dalla Legge 17 dicembre 2012, n. 221, ed implementato dal Decreto del Ministero dello Sviluppo Economico 21 febbraio 2013, si era introdotta una disciplina favorevole sotto il profilo fiscale per le c.d. start-up innovative[7], per tali intendendosi quelle società di capitali e cooperative, non

5 Le istruzioni operative per la corretta attuazione degli interventi in seguito alle novità normative intervenute nella disciplina dell'agevolazione per effetto della Legge di Bilancio 2017 sono emanate dal Ministero dello Sviluppo Economico con la circolare n. 14036/2017, successivamente modificata dalle circolari n. 17677/2017 e n. 22504/2017. Si rileva che per far fronte agli oneri derivanti dalla concessione dei contributi, la Legge di Bilancio 2017 ha rifinanziato la misura per complessivi 560 milioni di euro per l'anno 2018, 112 milioni di euro per ciascuno degli anni dal 2019 al 2021, 84 milioni di euro per l'anno 2022, 28 milioni di euro per l'anno 2023. Inoltre, in favore di questi investimenti è costituita una riserva pari al 20% del totale delle risorse finanziarie stanziate fino al 2023.

6 Il tema della *cybersecurity* è particolarmente di attualità all'interno del piano Industria 4.0. L'adeguamento dell'impresa alla versione 4.0 della sicurezza richiede l'individuazione delle difese dei sistemi sia da problemi interni che da attacchi esterni. Quest'ultimo aspetto dipende non solo dalla politica e dal livello di sicurezza dell'impresa, ma anche dalla sicurezza in generale dell'ambiente di rete e d'infrastruttura che circonda la stessa.

7 Come si può notare dalla Relazione Illustrativa al D.L. n. 179/2012, anche la normativa in tema di start-up innovativa si pone, tra le altre, la finalità di contribuire e rilanciare il progresso tecnologico e gli investimenti delle imprese in tal senso. Nella Relazione Illustrativa, difatti, si puntualizza che: "la disposizione individua nella crescita sostenibile, nello sviluppo tecnologico e nell'occupazione, in particolare giovanile, le finalità della sezione del decreto che disciplina le misure per la nascita e lo sviluppo di imprese start-up innovative.

quotate, di diritto italiano, e anche società europee residenti in Italia, che presentino una serie di requisiti obbligatori e cumulativi[8].

Con la Legge di Bilancio 2017 il Legislatore è intervenuto con decisione sulla disciplina introdotta dal D.L. n. 179/2012 (già in precedenza soggetta ad alcune modifiche dai provvedimenti di Riforma del 2014 e del 2015), apportando considerevoli modifiche alle disposizioni contenute nell'art. 29 D.L. n. 179/2012.

Nelle economie moderne, l'innovazione tecnologica rappresenta un fattore moltiplicativo per lo sviluppo. Le start-up si contraddistinguono per la loro capacità di veicolare e irrorare l'innovazione all'interno di un sistema economico. L'impatto è trasversale: tutti i settori produttivi sono incoraggiati ad accogliere le innovazioni tecnologiche introdotte dalle start-up. […] Le misure descritte in questa Sezione del decreto sono tese a uno sviluppo armonico dell'ecosistema delle start-up e coinvolgono tutti gli attori in esso operativi. Questo approccio sistemico permette un'azione su tutte le fasi del ciclo di vita di una start-up. Intervenendo sulla semplificazione, riducendo gli oneri, prevedendo una disciplina specifica dei rapporti di lavoro si mira a creare condizioni e strumenti favorevoli per la nascita di nuove start-up. Favorendo gli investimenti in start-up, di provenienza tanto da cittadini privati quanto da aziende, e sostenendo gli incubatori e gli acceleratori, si favorisce inoltre la progressiva crescita delle start-up".

8 Tali requisiti sono i seguenti: 1. la società deve essere costituita e svolgere attività d'impresa da non più di 5 anni (art. 25, comma 2, lett. b), D.L. n. 179/2912, come sostituito dall'art. 4, comma 11-*ter*, lett. a), del D.L. 24 gennaio 2015, n. 3, convertito dalla Legge 24 marzo 2015, n. 33), in quanto la qualifica di start-up innovativa ha natura temporanea e non definitiva; 2. la sede principale degli affari e degli interessi della start-up deve essere in Italia, o in uno degli Stati membri dell'Unione Europea o in Stati aderenti all'Accordo sullo spazio economico europeo, purché abbia una sede produttiva o una filiale in Italia (art. 25, comma 2, lett. c), D.L. n. 179/2012, come sostituito dall'art. 4, comma 1, lett. b), D.L. 24 gennaio 2015, n. 3, convertito dalla Legge 24 marzo 2015, n. 33); 3. la società per essere qualificata start up innovative non può avere un totale del valore della produzione annua superiore a 5 milioni di euro (art. 25, comma 2, lett. d), D.L. n. 179/2012); 4. la società non distribuisce e non ha distribuito utili (art. 25, comma 2, lett. e), D.L. n. 179/2012); 5. la società ha, quale oggetto sociale esclusivo o prevalente, lo sviluppo, la produzione e la commercializzazione di prodotti e servizi innovativi ad alto valore tecnologico (art. 25, comma 2, lett. f), D.L. n. 179/2012); 6. la società non è stata costituita da una fusione, scissione societaria o a seguito di cessione di azienda o di rami di azienda (art. 25, comma 2, lett. g), D.L. n. 179/2012); 7. la società possiede almeno uno dei seguenti requisiti: a. le spese in ricerca e sviluppo sono uguali o superiori al 15 per cento del maggiore valore fra costo e valore totale della produzione della start-up innovativa; b. impiego come dipendenti o collaboratori a qualsiasi titolo, in percentuale uguale o superiore al terzo della forza lavoro complessiva, di personale in possesso di titolo di dottorato di ricerca o che sta svolgendo un dottorato di ricerca o in possesso di laurea che abbia svolto, da almeno tre anni, attività di ricerca certificata presso istituti di ricerca ovvero, in percentuale uguale o superiore a due terzi della forza lavoro complessiva, di personale in possesso di laurea magistrale ai sensi dell' articolo 3 del regolamento di cui al decreto del Ministro dell'istruzione, dell'università e della ricerca 22 ottobre 2004, n. 270; c. sia titolare o depositaria o licenziataria di almeno una privativa industriale relativa a una invenzione industriale, biotecnologica, a una topografia di prodotto a semiconduttori o a una nuova varietà vegetale ovvero sia titolare dei diritti relativi ad un programma per elaboratore originario registrato presso il Registro pubblico speciale per i programmi per elaboratore, purché tali privative siano direttamente afferenti all'oggetto sociale e all'attività di impresa (art. 25, comma 2, lett. h), D.L. n. 179/2012).

Più nel dettaglio, con la nuova normativa, la misura della detrazione dell'imposta lorda per i soggetti passivi IRPEF e per i soggetti passivi IRES è aumentata al 30%[9], mentre per il quadriennio 2013/2016, «le persone fisiche che abbiano investito, direttamente o indirettamente, in start-up innovative hanno potuto beneficiare di una detrazione IRPEF pari al 19% dell'investimento, con il vincolo di mantenerlo per almeno un biennio (a pena di decadenza dal beneficio)» (MOLINARO, 2017). La Legge di Bilancio 2017 ha previsto che, a decorrere dall'anno 2017, l'investimento massimo detraibile sia aumentato a 1 milione di euro[10] e che il termine minimo di mantenimento dell'investimento detraibile passi da due a tre anni.

Ancora, il Legislatore, nella redazione della Legge di Bilancio 2017 si è occupato di modificare in modo più favorevole al contribuente il credito d'imposta per attività di ricerca e sviluppo[11], introdotto dall'art. 3, D.L. 23 dicembre 2013, n. 145.

In particolare, secondo quanto disposto dall'art. 1, commi 15 e 16 della Legge di Bilancio 2017, il periodo di tempo nel quale possono essere effettuati gli investimenti in attività di R&S ammissibili ai sensi di quanto previsto dalla normativa di riferimento viene esteso di un anno (fino al 31 dicembre 2020 in luogo del 31 dicembre 2019). Inoltre, a decorrere dal 2017, la misura dell'agevolazione è elevata al 50% per tutte le categorie di spesa. Peraltro, sono ormai ammissibili le spese relative a tutto il personale impiegato nelle attività rilevanti, essendo venuto meno il requisito del "personale altamente

9 Come sancito dall'attuale art. 29, comma 7-*bis*, D.L. n. 179/2012, introdotto dall'art. 1, comma 66, lett. c), Legge 11 dicembre 2016, n. 232.

10 Come previsto dall'attuale art. 29, comma 3-*bis*, D.L. n. 179/2012, introdotto dall'art. 1, comma 66, lett. a), Legge 11 dicembre 2016, n. 232.

11 Si rammenta che la misura agevolativa consiste nel riconoscimento di un credito d'imposta, utilizzabile esclusivamente in compensazione, pari al 25% delle spese di ricerca e sviluppo incrementali rispetto ad una media fissa di riferimento (media dei medesimi investimenti effettuati nel triennio 2012-2014), a fronte di un investimento minimo pari a 30.000 euro. Nell'ambito delle spese agevolabili si annoverano quelle relative a: 1. personale altamente qualificato impiegato in attività di ricerca e sviluppo; 2. quote di ammortamento di strumenti e attrezzature di laboratorio; 3. ricerca *extra-muros*; 4. competenze tecniche e privative industriali. Per le spese di cui ai numeri 1 e 3, poi, l'agevolazione si applicava in misura maggiorata del 50% delle spese sostenute. Per maggiori informazioni circa le modalità applicative del credito d'imposta per attività di ricerca e sviluppo, cfr. la circolare n. 5/E 2016 dell'Agenzia delle Entrate.

qualificato". Assume notevole importanza, poi, quella modifica normativa secondo la quale il credito d'imposta può essere utilizzato anche dalle imprese residenti o dalle stabili organizzazioni nel territorio dello Stato di soggetti non residenti che effettuino le attività di ricerca dietro commissione di imprese residenti o localizzate in altri Stati membri dell'Unione Europea, negli Stati aderenti all'accordo sullo Spazio Economico Europeo ovvero in Stati che consentono un adeguato scambio di informazioni secondo le convenzioni e i trattati contro le doppie imposizioni.

Occorre notare, altresì, che l'importo massimo annuale del credito d'imposta riconosciuto a ciascun beneficiario viene elevato da 5 a 20 milioni di euro.

Infine, per concludere questa panoramica degli strumenti introdotti dal Legislatore tributario per dare un deciso impulso all'innovazione tecnologica delle imprese, non può che menzionarsi il Patent Box, agevolazione fiscale introdotta dall'art. 1, commi 37-45, Legge 23 dicembre 2014, n. 190 (Legge di Stabilità 2015), modificato dall'art. 5, D.L. 24 gennaio 2015, n. 3 (Misure urgenti per il sistema bancario e gli investimenti), c.d. Decreto *Investment Compact*. Le disposizioni attuative della normativa in esame sono state emanate con decreto ministeriale del Ministro dello Sviluppo Economico di concerto con il Ministro dell'Economia e delle Finanze in data 30 luglio 2015 (c.d. Decreto Patent Box). Inoltre, la normativa primaria è stata modificata dalla L. 28 dicembre 2015, n. 208, ossia dalla Legge di Stabilità 2016. La disciplina del Patent Box è stata altresì oggetto di interpretazione da parte dell'Agenzia delle Entrate in due diverse occasioni, ossia nella Circolare 1 dicembre 2015, n. 36/E, e nella Circolare 7 aprile 2016, n. 11.

Il Patent Box italiano non costituisce un *unicum* nel panorama europeo, poiché molti Paesi hanno introdotto, ormai da qualche anno, la medesima agevolazione fiscale (si pensi, ad esempio, al Belgio, al Regno Unito, al Lussemburgo o anche ai Paesi Bassi). Peraltro, esso è stato di recente oggetto di indagine da parte dell'OCSE che, con l'Azione 5 del Progetto BEPS (*Base Erosion and Profit Shifting*) ha delimitato l'ambito di operatività di tale

strumento, in ragione della sua potenziale capacità di distorcere il mercato, e ne ha definito alcuni criteri e parametri applicativi[12].

Il Patent Box consente di ottenere un'agevolazione fiscale (ossia un'esenzione pari al 30% per il 2015, 40% per il 2016 e 50% dal 2017 in poi) per i redditi che i soggetti esercenti attività d'impresa ritraggono dall'utilizzo, diretto o indiretto, di un bene immateriale, a patto che tali soggetti siano in grado di dimostrare che vi sia una relazione tra i costi sostenuti e il reddito ottenuto, mediante una formula che ricalca in maniera evidente quella suggerita dall'OCSE nel Progetto BEPS in precedenza menzionato. L'agevolazione può essere riconosciuta solo in seguito all'esercizio della relativa opzione (irrevocabile e rinnovabile) da parte dell'impresa, e può avere durata non superiore a cinque anni.

Una volta delineati brevemente alcuni profili essenziali di quegli strumenti elaborati dal Legislatore, testimonianze di uno sforzo sempre maggiore per rilanciare, almeno dal punto di vista della politica fiscale, lo sviluppo delle imprese in chiave tecnologica, è possibile affrontare il tema dell'iperammortamento.

3. L'iperammortamento. L'iperammortamento è indubbiamente una delle più importanti e rilevanti agevolazioni introdotte dalla Legge di Bilancio, la cui dicitura richiama il superammortamento, ovverosia la maggiorazione, ai soli fini fiscali, per i nuovi beni strumentali acquistati tra il 15 ottobre 2015 e il 31 dicembre 2016, del 40% del valore del bene ammortizzabile (quindi 140% del totale acquistato). La Legge di Bilancio 2017, oltre a prorogare l'applicazione

12 Il capitolo quarto ("*Revamp of the work on harmful tax practices: Substantial activity requirement*") del BEPS Action Plan 5 ("*Countering Harmful Tax Practices More Effectively, Taking into Account Transparency and Substance*") si pone quale obiettivo quello di limitare gli eventuali effetti perniciosi di talune pratiche fiscali e di alcuni strumenti agevolativi adottati dagli ordinamenti giuridici. In particolare, osserva l'OCSE, taluni incentivi fiscali, che mirano allo sviluppo dei beni immateriali, spesso risultano oggetto di continui e costanti abusi da parte delle imprese. Pertanto, in merito al Patent Box, l'OCSE raccomanda ai Paesi che si sono dotati (o intendono dotarsi) di tale agevolazione fiscale, di introdurre un criterio di collegamento tra le spese sostenute per la creazione e lo sviluppo del bene immateriale e il reddito prodotto attraverso il suo sfruttamento (c.d. *nexus ratio*). Inoltre, l'OCSE individua le tipologie di beni immateriali che non possono essere oggetto del regime fiscale in esame.

del superammortamento ai beni materiali strumentali acquistati fino al 31 dicembre 2017, e ad estendere tale strumento anche ad altre tipologie di beni, ha introdotto una normativa che permetterà di favorire gli investimenti nell'automazione e nell'utilizzo delle nuove tecnologie.

Prima di analizzare l'iperammortamento, tuttavia, sembra opportuno, per ragioni di completezza, sintetizzare gli aspetti più caratteristici e peculiari del superammortamento.

Per ciò che riguarda il suo ambito soggettivo, la legge di Stabilità per il 2016 prevedeva che il superammortamento spettasse ai soggetti titolari di reddito d'impresa e agli esercenti arti e professioni, per gli investimenti effettuati tra il 15 ottobre 2015 e il 31 dicembre 2016.

Come chiarito nella Circolare n. 23/E/2016 dall'Agenzia delle Entrate, possono beneficiare del superammortamento tutte le imprese, indipendentemente dalla natura giuridica, dalla dimensione e dal settore economico in cui operano, ed i titolari di reddito di lavoro autonomo, restando «escluse le persone fisiche che applicano il regime forfetario» (BALZANELLI – VACARENGHI, 2017). Viceversa, come correttamente osservato da parte della dottrina, l'agevolazione del «superammortamento viene applicata anche ai soggetti che hanno aderito al regime dei minimi *ex* D.L. n. 98/2011» (P. MENEGHETTI, V. MENEGHETTI, 2016), ossia coloro cui viene applicata l'imposta sostitutiva del 5%. La stessa Amministrazione Finanziaria, con la Circolare n. 4/E/2017, ha esteso il regime del superammortamento anche alle imprese residenti all'estero, «purché dotate di una stabile organizzazione nel territorio dello Stato» (FORMICA –ALIBERTI, 2017). Come si è in precedenza menzionato, l'agevolazione fiscale in oggetto spetta in relazione ai beni strumentali acquistati fino al 31 dicembre 2017. La Circolare n. 23/E/2016 dell'Agenzia delle Entrate ha confermato che il superammortamento spetta in capo all'acquirente anche in relazione ai beni esposti in show room. Come osservato da attenta dottrina, dunque, «l'agevolazione non spetta per i beni utilizzati dal rivenditore per finalità diverse dalla mera esposizione, come nel caso

dell'autovettura immessa su strada dal concessionario, anche solo per scopi dimostrativi» (ALBANO, 2016).

L'agevolazione fiscale in esame, in conseguenza e per l'effetto della Legge di Bilancio 2017, è estesa agli investimenti effettuati da imprese e professionisti fino al 31 dicembre 2017, ovvero anche oltre tale data, ma entro il 30 giugno 3018, a condizione che entro fine 2017 sia confermato l'ordine inviato al fornitore e sia versato un acconto almeno pari al 20% del costo di acquisizione.

Si ricorda, poi, che al fine di incentivare lo sviluppo dell'innovazione, il legislatore della Legge di Bilancio 2017 ha esteso, a certe condizioni, la maggiorazione del 40% anche ad alcune tipologie di beni immateriali (art. 1, comma 10). In merito a quest'ultima maggiorazione, appare doveroso sottolineare che i beni materiali e immateriali devono rispettare anche il requisito dell'interconnessione. Pertanto, come puntualizzato da una certa dottrina, «la maggiorazione del 40% del costo di acquisizione dei beni immateriali spetta a condizione che l'impresa abbia acquisito almeno un bene materiale che beneficia dell'iperammortamento, anche se non collegato con i detti beni immateriali» (FERRANTI, 2017). In caso di acquisizione di un *software* la maggiorazione si applica a condizione che lo stesso sia *stand alone* (cioè non necessario per il funzionamento di un bene materiale): in caso contrario il *software embedded* è agevolato con l'iperammortamento spettante per il bene materiale in cui è integrato. Occorre altresì precisare che il beneficio spetta anche se il *software* è acquistato a titolo di licenza d'uso[13].

13 Si precisa, altresì, che secondo la Circolare n.8/E/2017 dell'Agenzia delle Entrate, "affinché un bene, coerentemente con quanto previsto dall'art. 1, comma 11, della legge di bilancio 2017, possa essere definito interconnesso ai fini dell'ottenimento del beneficio dell'iperammortamento del 150%, è necessario e sufficiente che: 1. scambi di informazioni con sistemi interni (es.: sistema gestionale, sistemi di pianificazione, sistemi di progettazione e sviluppo del prodotto, monitoraggio, anche in remoto, e controllo, altre macchine dello stabilimento, ecc.) e/o esterni (es.: clienti, fornitori, partner nella progettazione e sviluppo collaborativo, altri siti di produzione, *supply chain*, ecc.) per mezzo di un collegamento basato su specifiche documentate, disponibili pubblicamente e internazionalmente riconosciute (esempi: TCP-IP, http, MQTT, ecc.); 2. sia identificato univocamente, al fine di riconoscere l'origine delle informazioni, mediante l'utilizzo di standard di indirizzamento internazionalmente riconosciuti (es.: indirizzo IP). In altri termini, il 140% di ammortamento spetta ai *software*, sistemi, piattaforme e applicazioni per la produzione automatizzata e intelligente, caratterizzata da elevata capacità cognitiva, interazione e

Dopo questa breve descrizione di alcuni aspetti salienti del superammortamento, è possibile delineare i tratti più significativi e innovativi dell'iperammortamento.

Tale disciplina si applica, in particolar modo, ai beni caratteristici della c.d. quarta rivoluzione industriale che rientrano nelle categorie inserite nell'allegato A della Legge di Bilancio 2017 (come, ad esempio, investimenti in *cybersecurity*, *big data*, *cloud*, robotica industriale, manifattura digitale e banda ultra-larga[14]), e introduce una maggiorazione del 150% del valore del bene ammortizzabile rispetto al costo storico (ovverosia il 250% del totale acquistato).

La più attenta dottrina ha notato, dunque, che «la Legge n. 232/2016 premia in misura differenziata (150% e 40%) l'acquisto di macchinari "intelligenti" e quello di *software*» (BALZANELLI - VALCARENGHI, 2017). Sono, viceversa, esclusi dall'agevolazione in esame i fabbricati e le costruzioni nonché gli altri beni per i quali sono stabiliti coefficienti di ammortamento inferiori al 6,5%, ai sensi del D.M. 31 dicembre 1988.

Come è agevole notare, beneficiarie di questa *nuova* agevolazione sono, in special modo, le imprese che operano nel settore industriale della sicurezza informatica, nanotecnologie, *big data*, meccatronica e robotica. La dottrina, in seguito ad un'analisi preliminare della nuova agevolazione fiscale, non ha ritenuto applicabili le disposizioni di derivazione comunitaria in tema di aiuti di Stato, in quanto essa è «rivolta alla generalità dei soggetti-imprese (sia come

---

adattamento al contesto, autoapprendimento e riconfigurabilità (*cybersystem*), ma anche a quelli per l'utilizzo lungo le linee produttive di robot collaborativi e macchine intelligenti per la sicurezza e la salute dei lavoratori, la qualità dei prodotti finali e la manutenzione predittiva. Sono agevolabili, peraltro, i *software* per la protezione di reti, dati, programmi, macchine e impianti da attacchi, danni e accessi non autorizzati (*cybersecurity*), nonché di *virtual industrialization* che, simulando virtualmente il nuovo ambiente e caricando le informazioni sui sistemi cyberfisici al termine di tutte le verifiche, consentono di evitare ore di test e di fermi macchina lungo le linee produttive reali.

14 Rientrano, ad esempio, nell'ambito del beneficio in esame i beni strumentali il cui funzionamento è controllato da sistemi computerizzati e/o gestito, tramite opportuni sensori e azionamento, i dispositivi per l'interazione uomo-macchina e per il miglioramento dell'ergonomia e della sicurezza del posto di lavoro in logica 4.0. Più in particolare, vi rientrano le macchine utensili, gli strumenti e i dispositivi per asportazione, operanti con laser e altri processi a flusso di energia, elettroerosione, processi elettrochimici, ecc.

categorie merceologiche, che come dimensioni o forma giuridica» (FAIENZA, 2017).

A differenza dei superammortamenti, l'iperammortamento non si applica agli esercenti arti e professioni. E ciò si desume dall'esplicito richiamo all'impresa, contenuto nell'art. 1, comma 11. L. di Bilancio 2017[15].

Inoltre, per la determinazione del *dies a quo* di effettuazione dell'investimento, si applicano le disposizioni in tema di principio di competenza di cui all'art. 109 TUIR. «La Circolare n. 4/E/2017 chiarisce che il momento di effettuazione degli investimenti – rilevante al fine di appurare la spettanza o meno della maggiorazione del 150% - deve distinguersi da quello dal quale è possibile fruire del beneficio in commento» (FORMICA – DE NICOLA, 2017). Tale dottrina ha ritenuto opportuno evidenziare che, quantomeno nel caso di beni agevolabili in proprietà, la maggiorazione in parola, potrà essere dedotta – ai sensi dell'art. 102 del TUIR – solo a partire dall'esercizio di entrata in funzione del bene, ovvero solo dalla medesima annualità fiscale dalla quale è possibile la deduzione ordinaria degli ammortamenti. Peraltro, in caso di bene materiale strumentale nuovo, inserito nell'Allegato A, e consegnato nel 2016, questo non può fruire della maggiorazione del 150%, poiché, in tale circostanza, l'investimento viene effettuato al di fuori del periodo agevolato.

Secondo la dottrina, appare particolarmente importante la precisazione che «l'istanza di interpello di cui all'art. 11 della Legge n. 212/2000 non può essere presentata per ottenere risposta in merito all'ambito oggettivo di applicazione dell'agevolazione e che in merito alla riconducibilità dei beni tra quelli indicati nell'allegato A i contribuenti devono acquisire autonomamente il

15 La norma, peraltro, stabilisce che per fruire di tale beneficio devono sussistere le seguenti condizioni: a) produzione da parte dell'impresa di una dichiarazione sostitutiva di atto notorio del legale rappresentante ai sensi del D.P.R. n. 445/2000; ovvero, b) per i beni aventi ciascuno un costo superiore a 500.000 euro, una perizia tecnica giurata rilasciata da un ingegnere o da un perito industriale iscritti nei rispettivi albi professionali o da un ente di certificazione accreditato. Nella Relazione Illustrativa alla Legge di Bilancio 2017 è stato precisato che "la dichiarazione del legale rappresentante e l'eventuale perizia devono essere acquisite dall'impresa entro il periodo di imposta in cui il bene entra in funzione ovvero, se successivo, entro il periodo di imposta in cui il bene è interconnesso al sistema aziendale di gestione della produzione o alla rete di fornitura […] in quest'ultimo caso, l'agevolazione sarà fruita solo a decorrere dal periodo d'imposta in cui si realizza il requisito dell'interconnessione".

parere tecnico del Ministero dello Sviluppo economico, limitandosi a conservarlo, senza presentare un'istanza di interpello all'Agenzia delle Entrate» (FERRANTI, 2017).

Il costo agevolabile del bene viene determinato ai sensi dell'art. 110 TUIR e, conseguentemente, al netto di eventuali contributi in conto impianti, a prescindere dalle modalità di contabilizzazione degli stessi. Secondo quanto chiarito dall'Agenzia delle Entrate, qualora in un periodo d'imposta si fruisca dell'agevolazione in misura inferiore al limite massimo consentito, il differenziale non dedotto non potrà essere recuperato in alcun modo nei periodi d'imposta.

Per ciò che riguarda il costo agevolabile, infine, la norma afferma che «la maggiorazione del 150 per cento si applica al costo di acquisizione, senza fare riferimento espresso – a differenza della disposizione relativa al superammortamento – alle quote di ammortamento e ai canoni di *leasing*» (FERRANTI, 2017).

4. Conclusioni. Orbene, giunti alla conclusione di questo breve scritto, è possibile apprezzare, in primo luogo, lo sforzo notevole che il Legislatore tributario ha sostenuto negli ultimi anni per cercare di rilanciare l'attività produttiva delle imprese. Ma, più nel dettaglio, si può notare la forte spinta in favore del progresso tecnologico delle imprese. E ciò che desta maggiore interesse, senza dubbio, è la possibilità di cumulare molti degli incentivi fiscali, salvo la sussistenza di espliciti divieti. E in questo senso si è espressa anche l'Agenzia delle Entrate con la Circolare n. 5/E/2016, «con la quale è stato chiarito che i costi ammissibili al credito d'imposta per attività di ricerca e sviluppo vanno assunti al lordo di eventuali contributi ed agevolazioni pubbliche ricevuti, a condizione che l'importo risultante dal cumulo non sia superiore al costo sostenuto, nel quale caso occorrerà ridurre corrispondentemente il credito d'imposta»[16] (SEPIO - SILVETTI, 2017).

16 Cfr. sul punto la Risoluzione n. 12/E/2017, nonché, in precedenza, la Risoluzione n. 66/E/2016.

Tuttavia, è ancora difficile stabilire se tali incentivi siano sufficienti per lanciare in maniera decisa il nostro Paese nella direzione di una trasformazione del tessuto imprenditoriale in chiave digitale, o se sia necessario elaborare altri strumenti che possano consentire questa innovazione in chiave Industria 4.0.

Riferimenti bibliografici

G. ALBANO, *Super-ammortamento con le regole generali del TUIR anche per i soggetti IAS*, in *Corriere Tributario*, 2016;
G. ALBANO, *Proroga del superammortamento e introduzione dell'iperammortamento per l'Industria 4.0*, in *Corriere Tributario*, 2016;
G. ANDREANI – A. TUBELLI, *"Super-ammortamento": nel primo anno un'agevolazione a metà*, in *Il Fisco*, 2016;
M. BALZANELLI – G. VALCARENGHI, *Differenze e analogie tra super e iper-ammortamenti*, in *Il Fisco*, 2017;
M. BALZANELLI – G. VALCARENGHI, *Super e iper-ammortamenti sotto la lente delle Entrate*, in *Il Fisco*, 2017, p. 807 e ss.;
A. M. FAIENZA, *Investimenti strumentali nuovi: aumentano gli incentivi*, in *Bilancio e reddito d'impresa*, 2017;
G. FERRANTI, *L'Agenzia delle Entrate chiarisce le modalità di calcolo dei maxi-ammortamenti*, in *Corriere Tributario*, 2016;
G. FERRANTI, *Chiarita la disciplina di iper e super-ammortamenti dei beni immateriali*, in *Corriere Tributario*, 2017;
G. FERRANTI, *L'Agenzia chiarisce la proroga del super-ammortamento dei beni strumentali nuovi*, in *Corriere Tributario*, 2017;
G. FERRANTI, *Le agevolazioni per i beni strumentali nuovi acquisiti in proprietà e in leasing a partire dal 2017*, in *Corriere Tributario*, 2017;
G. FORMICA – F. ALIBERTI, *Super-ammortamenti: l'Agenzia chiarisce la proroga e l'ampliamento dell'agevolazione*, in *Il Fisco*, 2017;
R. FRISCOLANTI – B. PAGAMICI, *Sabatini-ter, agevolazioni per investimenti 4.0*, in *Cooperative e enti non profit*, 2017;
R. FRISCOLANTI– B. PAGAMICI, *Legge di bilancio 2017: tutte le novità per cooperative ed enti non profit*, in *Cooperative e enti non profit*, 2017;
L. GAIANI, *Super e iper-ammortamento: pianificazione temporale degli investimenti da fare e/o da rinviare*, in *Il Fisco*, 2016;
P. MENEGHETTI – V. MENEGHETTI, *Requisiti ed effetti dei superammortamenti*, in *Corriere Tributario*, 2016;
G. MOLINARO, *Incentivi fiscali per le start-up innovative*, in *Corriere Tributario*, 2017;
G. SEPIO, *La cumulabilità degli incentivi legati a Industria 4.0*, in *Il Fisco*, 2017;
G. VALCARENGHI, *Super ammortamenti: beneficio fiscale per rilanciare gli investimenti*, in *Corriere Tributario*, 2015.

Prassi dell'Agenzia delle Entrate

Circolare 1 dicembre 2015, n. 36/E;
Circolare 16 marzo 2016, n. 5/E;
Circolare 7 aprile 2016, n. 11/E;
Circolare 26 maggio 2016, n. 23/E;
Circolare 20 marzo 2017, n. 4/E;

Circolare 7 aprile 2017, n. 8/E.
Risoluzione 3 agosto 2016, n. 66/E;
Risoluzione 13 aprile 2017, n. 12/E.

Prassi del Ministero dello Sviluppo Economico

Circolare 15 febbraio 2017, n. 14036;
Circolare 24 febbraio 2017, n. 17677;
Circolare 9 marzo 2017, n. 22504.

Fonti sovranazionali

OECD BEPS Action Plan 5: Countering Harmful Tax Practices More Effectively Taking into Account Transparency and Substance.

*La collaborazione tra imprese per la sicurezza informatica**

di **GIAN DOMENICO MOSCO**

SOMMARIO: **1.** LE DOMANDE. – **2.** I FATTORI RILEVANTI PER LA *CYBER SECURITY* DELLE IMPRESE: L'OPPORTUNITÀ DI UNA RISPOSTA IN *POOL*. – **3.** GLI STRUMENTI PER LA COLLABORAZIONE TRA IMPRESE: CONSORZI E CONTRATTO DI RETE. – **4.** IL CONSORZIO COME ALTERNATIVA ALL' *OUTSOURCING*. **5.** – *INFORMATION SHARING* E RAPPORTO TRA PUBBLICO E PRIVATO. – **6.** L'INFLUENZA DELL'INTELLIGENZA ARTIFICIALE SULLA *CYBER SECURITY*.

Abstract

The complexity and costs linked with *Cyber Security* represent real obstacles for businesses, especially the smaller ones. One way to overcome them is to cooperate in order to create information technology security systems. In Italy two different tools may be used for this goal: the *contratto di rete* (network contract) and, to a greater degree, consortiums.
Information sharing however requires a public intervention. A step in this direction has been undertaken by the EU, with the NIS directive 1148/2016 which paves the road for cooperation between public institutions and the private sector, mainly companies.
Artificial intelligence will interfere more and more with cyber security, generating risks and opportunities, which can already be foreseen.

1. Le domande. In questo breve intervento vorrei pormi tre domande e cercare di dar loro una prima risposta.

La prima e principale domanda è la seguente: le imprese per elevare i livelli di sicurezza informatica devono muoversi necessariamente da sole o vi sono ragioni – e si dispone di strumenti – per incrementare la *Cyber Security* attraverso forme di collaborazione e condivisione tra loro?

La seconda domanda riguarda più specificamene l'*Information Sharing* e il rapporto tra privato e pubblico alla luce, soprattutto, della direttiva 2016/1148 UE del luglio dell'anno scorso.

La terza e ultima domanda è: quale influenza avrà sulla *Cyber Security* il diffondersi dell'intelligenza artificiale e, se la avrà, sarà positiva o negativa?

2. I fattori rilevanti per la *Cyber Security* delle imprese: l'opportunità di una risposta in *pool*. Per cercare di rispondere alla prima domanda vorrei ricordare anzi tutto alcuni fattori di carattere sia generale, sia specifico che assumono rilievo ai fini della sicurezza informatica delle nostre imprese.

Il primo è che il nostro sistema imprenditoriale è notoriamente costituito soprattutto da PMI.

Per l'ISTAT le imprese fino a 10 dipendenti (le c.d. micro imprese) sono il 95% del totale (dati 2015). Per Confindustria e CERVED (rapporto PMI 2016) tra le sole società di capitali ed escludendo sia le grandi, sia le micro imprese si contano circa 112 mila piccole imprese (<50 addetti e fino a 10 milioni di euro di fatturato o attivo) e quasi 24 mila medie imprese (23.736) (< 250 addetti e fino a 150 milioni di euro di fatturato o 43 milioni di attivo).

La grandissima parte delle micro e delle piccole imprese ha difficoltà nel disporre di risorse economiche e organizzative sufficienti per consolidarsi, innovare, crescere.

Sotto il profilo della sicurezza informatica, le imprese minori sono un bersaglio privilegiato degli attacchi informatici, sia *random*, sia mirati, e per loro le conseguenze negative sono in proporzione ancora maggiori che per le grandi poiché il dato dimensionale accentua l'asimmetria informativa della vittima rispetto all'attaccante, in quanto per queste imprese è più difficile dotarsi di un sistema di protezione e così reagire ai danni, economici e reputazionali, causati da una violazione informatica.

Una ragione, forse la più importante, di questo stato di cose è rappresentata dai costi della sicurezza informatica, il secondo fattore da ricordare.

Il *Cybersecurity Report 2016* realizzato dal CIS-Sapienza e dal Laboratorio Nazionale di *Cybersecurity*, che rappresenta una tappa fondamentale del percorso evolutivo di sicurezza informatica per le nostre p.m.i., ha operato una difficile semplificazione del sistema dei controlli (il *Framework Nazionale di Cybersecurity* delineato dal *Cybersecurity Report*

2015), riuscendo a selezionare 15 misure protettive che possono definirsi «essenziali» per resistere, quanto meno, agli attacchi più comuni. Si tratta, in sostanza, di un sistema difensivo minimale ma imprescindibile.

Anche puntando a realizzare solo questo sistema difensivo di base i costi sono significativi, secondo il Rapporto stimabili in circa 41.000 euro in 5 anni per una micro impresa, in poco più di 100.000 euro nello stesso periodo per una media impresa, ricompresi in questa forbice (41-100) per una piccola impresa.

Il terzo fattore è la consapevolezza, messa in luce dal *Framerwork* Nazionale per la *Cybersecurity* 2016 che, anche per le imprese maggiori, una risposta di sicurezza informatica è bene che non sia in *outsourcing*, ma affrontata all'interno dell'impresa come espressione di una propria cultura di gestione del rischio *cyber*, la sola che può assicurare risultati ottimali.

Infine, va ricordato che sempre il Rapporto 2016 del CIS Sapienza sottolinea che molti attacchi informatici a grandi impese passano attraverso le PMI della loro filiera produttiva, fornitrici di beni e servizi.

In conclusione, ci sono diverse ragioni – dimensioni delle impese, costi della sicurezza, inconvenienti della esternalizzazione, trasmissibilità lungo la filiera degli attacchi – che spingono nella direzione di una risposta in *pool* ai problemi di sicurezza informatica delle imprese, certamente di quelle più piccole ma anche, con loro, di quelle grandi o medie al vertice di una filiera.

3. Gli strumenti per la collaborazione tra imprese: consorzi e contratto di rete. Per agevolare il diffondersi della sicurezza informatica tra le imprese va dunque incentivata la collaborazione tra imprese.

Non mancano nel nostro ordinamento gli strumenti, contrattuali e organizzativi, utilizzabili dalle imprese per collaborare e affrontare senza ulteriori rinvii la questione della sicurezza informatica con costi accettabili, realizzando un sistema di controlli *cyber* che risponda almeno al modello "essenziale" delineato dal *Cybersecurity Report 2016*.

Due sono gli strumenti d'elezione per la collaborazione tra imprese che già hanno un'ampia diffusione, specie tra le piccole e medie imprese.

Anzi tutto, il consorzio tra imprenditori. Si tratta di uno strumento che prevede l'istituzione di un'organizzazione comune e che lascia ampio spazio all'autonomia contrattuale nel configurare la *governance* secondo le concrete esigenze delle imprese. Il codice civile prevede infatti un ordinamento interno corporativo, con un organo di tipo assembleare e uno di gestione, ma fortemente semplificato rispetto a quello di una società di capitali o cooperativa.

Allo stesso tempo il consorzio con attività esterna beneficia della limitazione della responsabilità patrimoniale (art. 2615, comma 1, c.c.), senza particolari vincoli quanto a fondo comune (che non deve avere un ammontare minimo) e controlli interni ed esterni. Insomma, uno strumento agile, sufficientemente sicuro e ben collaudato (MOSCO, 2017).

Il secondo strumento, più recente, è il contratto di rete, una figura contrattuale introdotta dall'art. 3, comma 4-*ter*, della legge 9 aprile 2009, n. 33, di conversione del d.l. 10 febbraio 2009, n. 5, poi ripetutamente modificato dal legislatore.

Il ricorso al contratto di rete è consigliabile soprattutto se non si vuole dar vita a un nuovo soggetto di diritto (anche se possono essere costituite reti entificate), ma limitare la collaborazione sul versante C*yber Security* alla messa in comune di informazioni o alla predisposizione di strumenti di difesa regolati solo sul piano contrattuale istituendo, se occorre, un fondo e un rappresentante comune (IAMICELI, CAFAGGI, MOSCO, 2013)

In definitiva, uno strumento adatto, anche per via di una disciplina normativa non del tutto convincente, per una prima collaborazione, non troppo intensa e impegnativa.

4. Il conosorzio come alternativa all'*outsourcing*. Vorrei chiarire a questo punto perché ho incluso il superamento dell'*outsourcing* tra le ragioni che spingono verso network imprenditoriali nel campo della *Cybersecurity*.

Credo che ci sia una terza via tra una gestione interna del rischio informatico e una sua esternalizzazione: per l'appunto, il ricorso a un consorzio (o a una rete) che possano offrire un approccio culturale alla Cybersecurity e valutazioni e presidi di sicurezza analoghi alla prima, ma con risparmi anche superiori alla seconda.

Del resto, agire in *pool* può consentire di andare oltre alle «misure essenziali di sicurezza» per muovere con decisione lungo il «percorso virtuoso» ipotizzato dal Rapporto 2016 del CIS, mettendo in atto «norme di sicurezza via via più complesse e articolate». E questo non solo affidandosi ancora al consorzio o alla rete, ma anche affiancando al sistema di controllo «essenziale», condiviso con le altre imprese, misure difensive realizzate dalla singola impresa, più evolute e calibrate sul proprio profilo di rischio.

Se per le imprese più grandi il tema della *Cybersecurity* è ormai uno dei più importanti e ricorrenti tra quelli oggetto d'esame da parte dei consigli di amministrazione, è auspicabile che ogni imprenditore, ogni organo amministrativo avverta come ricompreso tra i propri doveri quello di predisporre un assetto organizzativo adeguato anche con riguardo alla sicurezza informatica.

5. *Information Sharing* e rapporto tra pubblico e privato. Vorrei ora provare a rispondere alla seconda domanda.

È evidente, anzitutto, che la condivisione delle informazioni in relazione ad attacchi e minacce informatiche è, forse, la prima tappa di un *network* di imprese, consentendo di avere più informazioni a minor costo, interne ed esterne alla rete, di realizzare archivi comuni, ovviamente con caratteri di neutralità concorrenziale e garanzia di riservatezza, di mettere in campo a costi condivisi analisti capaci di prevenire, sulla base delle esperienze del passato, gli attacchi del futuro (CONSORZIO CINI, 2015).

La C*yber Security* richiede però un campo d'azione dei «difensori» molto ampio e ben coordinato con un *Information Sharing* non lasciato solo a iniziative volontarie e circoscritte.

In questo senso mi pare vada, a livello europeo, la recente direttiva europea c.d. NIS – la 2016/1148 del 6 luglio 2016 – che chiede a ciascun stato membro di dotarsi di una strategia nazionale di C*ybersecurity* che definisca obiettivi strategici, politiche adeguate e misure di regolamentazione nonché uno o più *team* (c.d. CSIRT) responsabili del monitoraggio degli incidenti nazionali e che forniscano allarmi tempestivi e diffondano informazioni su rischi e incidenti.

Mi limito a ricordare che il funzionamento del sistema si basa proprio su un meccanismo di *Information Sharing* basato su un *obbligo* di notifica degli incidenti significativi a carico degli operatori di servizi essenziali (le imprese pubbliche o private che gestiscono le c.d. «infrastrutture critiche») e dei fornitori di servizi digitali (mercati on-line, servizi di cloud e motori di ricerca).

Vi è però anche la *facoltà* di notifica da parte delle altre imprese e degli utenti informatici, dunque su base volontaria, «degli incidenti aventi un impatto rilevante sulla continuità dei servizi da loro prestati», posto che la loro conoscenza può essere di pubblico interesse e che il loro trattamento non rappresenta necessariamente un onere sproporzionato o eccessivo.

La direttiva 2016/1148 valuta infatti le informazioni sugli incidenti «sempre più preziose per il pubblico in generale e per le imprese, in particolare le piccole e medie imprese» e incoraggia il segretariato della rete di CSIRT a gestire un sito o una pagina web per mettere a disposizione del pubblico le informazioni sui principali incidenti che si verificano nell'Unione, «con particolare attenzione agli interessi e alle esigenze delle imprese» (considerando 40).

6. L'influenza dell'intelligenza artificiale sulla *Cyber Security*. L'ultima questione sulla quale, come ho anticipato, vorrei interrogarmi, limitandomi a qualche considerazione assai semplice, è il ruolo dell'Intelligenza Artificiale con riguardo alla C*yber Security*.

Ormai è sicuro che sempre più attività saranno affidate alla I.A. e alla robotica. Già oggi, per fare solo qualche esempio, è noto che si usano algoritmi per lanciare notizie (così fanno, per esempio, Agenzie quali Reuters o

Associated Press), per valutare il merito creditizio o i candidati a un posto di lavoro, per costruire modelli predittivi di atti terroristici o identificare sui *social media* i profili dei possibili terroristi, per definire strategie di investimenti e, sempre più spesso, per effettuarli. Sperimentazioni e prime applicazioni, anche con robots e alcune già consolidate, si registrano nei campi della medicina e delle professioni, in alcuni paesi della stessa giustizia.

Sempre maggiore, allora, sarà il rischio di subire attacchi a sistemi che agiscono, nonostante il riferimento all'intelligenza, sia pure artificiale, su base automatica e non «intelligente», utilizzando degli algoritmi che possono essere falsati o mandati in tilt.

Ne deriva la necessità di aumentare i livelli di protezione dalle minacce informatiche lasciando un ruolo fondamentale alla I.U., agli uomini, perché, come da più parti si sottolinea, le decisioni fondamentali e il controllo dei sistemi digitali hanno bisogno dell'intelligenza umana, di una *vera* intelligenza.

Allo stesso tempo, è evidente che i sistemi di I.A. possono dare una grossa mano nella lotta ai pirati informatici attraverso lo sviluppo di algoritmi capaci di adattare il sistema alle dinamiche dell'ambiente nel quale operano e di tener conto dell'esperienza maturata, il c.d. *deep learning* (pure a sua volta, evidentemente, fonte di pericoli). Il che può consentire non solo di analizzare velocemente quantità enormi di dati, ma di anticipare gli attacchi informatici o almeno di rispondervi velocemente.

*Intervento al Convegno "*Cybersecurity: una sfida per trasformare un rischio in opportunità per le PMI*", organizzato a Roma il 25 maggio 2017 da UNINDUSTRIA.

Riferimenti bibliografici

F. CAFAGGI, P. IAMICELI E G.D. MOSCO [2012], *Gli ultimi interventi legislativi sulle reti*, in *Il contratto di rete per la crescita delle imprese*, a cura di F. Cafaggi, P. Iamiceli, G.D. Mosco, Milano, p. 489 ss.

CIS SAPIENZA E CONSORZIO CINI [2016], *2015 Italian Cyber Security Report. Un Framework Nazionale per la Cyber Security*, 4 febbraio 2016, disponibile all'indirizzo *www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf*

CIS SAPIENZA E CONSORZIO CINI [2017], *2016 Italian Cyber Security Report. I controlli essenziali di sicurezza in un ecosistema cyber nazionale*, 2 marzo 2017, disponibile all'indirizzo *www.cybersecurityframework.it/sites/default/files/csr2016web.pdf*

CONFINDUSTRIA E CERVED [2016], *Rapporto PMI 2016,* disponibile all'indirizzo *https://know.cerved.com/it/studi-e-analisi/rapporto-cerved-pmi-2016*
CONSORZIO CINI [2015], *Il futuro della Cyber Security in Italia. Un libro bianco per raccontare le principali sfide che il nostro Paese dovrà affrontare nei prossimi cinque anni*, aa cura di R. Baldoni e R. de Nicola, disponibile all'indirizzo *https://www.consorzio-cini.it/index.php/it/labcs-home/libro-bianco*
ISTAT [2015], *Struttura e competitività del sistema delle imprese industriali e dei servizi – Report anno 2013*, 9 dicembre 2015, disponibile sul sito www.istat.it
G.D. MOSCO [2017], *Consorzi per il coordinamento della produzione e degli scambi*, in *Commentario del codice civile Scialoja-Branca-Galgano,* Bologna, 2017

Sezione Seconda:Digital Privacy & Artificial Intelligence

Governing Artificial Intelligence

di **TULIO ROSEMBUJ**

SUMMARY: **1.** THE BASICS. – **2.** THE BIG DATA: FROM COGNITIVE TO SURVEILLANCE. – **3.** THE ALGOROTHMIC SOCIETY. – **4.** ALGORITHMIC PRINCIPLES. **5.** – ABOUT THE GOVERNANCE COMMON PRONCIPLES.

"I think we should be very careful about artificial intelligence.If I had to guess at what our biggest essential threat is, it´s probably that…I `m increasingly inclined to think there should be some regulatory oversight,maybe at the national and international level, just to make sure that we don't` do something very foolish."(*Elon Musk).*
(Aileen Graef, Elon Musk:We are "Summoning a Demon" with Artificial Intelligence, UPI,October 27,2014).

1. The basics. *Marvin Minsky* defines artificial intelligence as "the science of making machines do things that would require intelligence if done by (people)."

There is a machine, a device, an artifact doing things that represents tasks to be performed and goals to be obtained; which, at some grade, will be similar to human acts.

Beyond the metaphors, which may be more or less appropriate – the machine is not a human being-, the fact is that there are computational processes formulated as computer programs, capable of communication, representing knowledge and carrying out automatic analysis to reach conclusions. The computer program needs to get data, find patterns, and do predictions to achieve its programmed outcome.

Soshana Zuboff observed that information technology has a duality which she calls "computer mediated", and it means automation and information at the same time. The computer, in this sense, is not only the medium of information but it also produces information.

The algorithm is the core of this computer process and computer programs, which means a specific sequence of logical operations that provides step- by-step instructions for computers to act on data and take predetermined

automated decisions. The outcomes are based on data inputs and decisional parameters.

Artificial intelligence is a computer program – an algorithm- that makes and executes decisions in response to external circumstances, (LYNN M.LOPUCKI*).*

The algorithm could change in response to its output and improve with the experience, learning with data, or extracting patterns from data. Machine learning is a statistical process that starts with a bulk of data and tries to derive a rule or a procedure that explains the data or can predict future data.

The definition is clear: “Machine learning algorithms can figure out how to perform important tasks by generalizing from examples “. (PEDRO DOMINGOS, 2013*).*The machine is not able to self-program, but it could be prepared to generate and store associations and facts from the data. The generalization means the capability to associate in timely fashion based on limited data.The generalization implies some kinds of presumptions which can drive to the repetition of past mistakes(e.g. criminal activity) or effects which were not intended to assume(e.g., unfair discrimination). The interpretation and prediction rules show one of the main problems in artificial intelligence, due to the fact that outcomes could be influenced by the programmers and then the conclusions become arbitrary or disparate, contaminated by the “beliefs, fallibilities, and biases of the person who created them.”(L.BARRET, 2016*)*

One of the main characteristics in machine learning is the so called deep learning. Deep learning uses learning techniques combining layers of neural networks to identify the profiles of a data set that are necessary to make decisions. There are many layers between input and output data and the outputs from the previous layers are inputs for the next (artificial neural network). (JERRY KAPLAN, 2016*).*

Machine learning and deep learning algorithms are the last frontier of artificial intelligence and are used in Web search, spam filters, credit scoring, insurance risk, fraud detection, stock trading, drug design, employment evaluations, health records, hiring searches, housing, and many other

applications. In addition, artificial intelligence agents that have the physical support and interact with the environment a machine “capable of performing tasks by sensing its environment and/or interacting with external sources and adapting its behavior” (*EN ISO 8373)*

The emergence of such robots are occupying sensitive and perhaps dangerous spaces that were previously occupied by human beings. We now have robot killers (military drones), robot cars, health robots, home robots, which all share common features: they may have access through their sensors, to a large and uncontrolled volume of information; they are ordinarily connected to the cloud and become big consumer of personal data and operate on the people behavior.

The best example are the autonomous weapons that would select and engage targets without meaningful human control. This shows the absence of appropriate regulation on artificial intelligence in general and over its agents in particular. There are not international legally binding instruments or even national laws prohibiting the development, production and use of the so called killer robots.

M.R.Calo exposes the raise of robots and privacy concerns. First, in terms of direct surveillance on the persons; second, the access to historically protected spaces-home robots-; and, third, and more dangerous, the social meaning, implicating what he called “ setting privacy”, or, the description of how a person programs and interact with a robot in his or her intimacy.

The robot is the avatar on earth, a player of virtual world in the real world. As we know an avatar is the physical representation of the player in the virtual world, used to co-inhabit simultaneously and interact with others players’ avatars. Now, we have a physical avatar in the real world interacting under human programs with others agents and adapting its behavior. We can say that the robot is an avatar in the real world. The risk and the threat is obvious.The avatar has no limits, moral, feelings, conscience, intentionality, other than the planned use of the algorithms, the time to use them and the purpose planned by humans.

2. The big data: from cognitive to sourveillance. Data is the foundation of artificial intelligence. It is the principal raw material of the algorithm, like cotton, wheat or fuel in the last century.

Data processing is the digital and virtual essence: without data there is no algorithm and without algorithm it is difficult to argue that there is artificial intelligence, digital goods or virtual goods. The value of data lies in its infinite reuse "the data's value is calculated on the basis of all the possible ways in which it could be used in the future and not merely on the basis of its present use"(V.MAYER-SCHONBERGER,K.CUKIER*)*

The recombination of data, its accumulation and its extension are its real value and therefore the impulse for its accumulation by the organizations like *Facebook, Twitter, Amazon, Visa, MasterCard, Bloomberg* and the like.

The initial data is susceptible to be eternal, reiterated and repeated continuously and systematically applied. Should that be personal data, she will lose track of her identity by the deprivation of personal rights.

D.J.Solove highlights privacy, because it is the protector of personal interests, above all, of society, before that of the individual. Privacy is not a fight for personal interest against social interest, but the protection of the individual on the basis of society's own values. "You cannot fight for an individual right against the more important social good. Questions of privacy involve a balance of social interests on both sides of the scale".

S.Rodota focuses its critical concern on the fact that data, by its spread use and reuse suggests that the identity of individuals "is built by others". The problem is not only the construction of profiles but the future use of algorithm, treated with "probability techniques which constructs a hypothetical distorting identity". Further to the reconstruction of new personal identities, these could not be the same as the initial ones.

The algorithm builds an identity through some kind of classification which is the result of programs created by humans that go beyond rationality and become manipulation or monitoring, without any transparence.

The algorithm provides generalization and prediction from the extraction, storage, and analysis of data, creating correlations, almost without evidence. Data mining is the process which takes place to define artificial intelligence as rational behavior. However, the identification of predictive algorithms with rational action cannot be the best solution because they are usually developed by somebody with a clear intention of profit or governance.

The rationale behind the algorithmic decision making is essentially opaque, secret, and few know how it works.

Big Data is the fuel that runs the algorithm success. “Collection and processing of data produces ever more data, which in turn, is used by algorithms to improve themselves. Based on Kant’s famous statement, algorithms without data are empty; data without algorithms are blind.”(J.M.BALKIN, 2015)

Y.Moulier Boutang coined the term *cognitive capitalism* and *S.Zuboff* qualified the process as *surveillance capitalism*. The surveillance, access and control becomes the core of the system, through the, collection, extraction, storage and analysis by big data. It is likely that surveillance provides a better description of what is actually happening. Many scholars use the concept of surveillance as the major threat of artificial intelligence, together with access and control.

Data flows from sources through very well-known ways, providing huge amounts of statistical raw material information on social, economic, financial, consumer, climate, genomic trends and human behavior. First of all, there was e-commerce, Internet transactions and the mere access to Internet. Second, the flows collected through artificial intelligence devices, sensors, agents placed in a wide range of objects and persons. Third, the flows from the banking system, credit rating agencies, credit cards, airlines, health care, insurance, telecommunications companies and government databases on climate,

genomic, or taxation. Fourth, the flows from public cameras on the streets, shops, public and private buildings and not least the smartphones. Finally, the individual attraction for entertainment, consumption, use or mere information of digital goods, books, films, music - or digital and personal needs (*Facebook).*

"Big Data is constituted by capturing small data from individuals computer mediated actions and utterances in their pursuit of effective life" (S.ZUBOFF, 2017*).* This last source it is very important. Personal data is the essential resource for the digital economy and it is "unpaid work" (P.COLLIN-N.COLIN, 2013*).* Personal data is the most valuable currency of the millennium. The unpaid work of users is probably the most important source of profits by large companies providing Internet content.

The free contributions from users to the digital economy illustrate the extraordinary increase in profits. Users without remuneration incorporate originality in the co-creation of the applications of the artificial intelligence software, fueling their exponential returns.

J.Lanier affirm that digital designs do not treat people as special, but as necessary elements in a larger machine of information. However, people are the only source and target of information; the unique meaning of the artificial intelligence. He proposes that the organizations have to pay people for the information collected if that information is found to be valuable. That includes financial technology schemes such as high frequency trading, search engines of social networks, insurance and intelligence agencies.

This is, for now wishful thinking. In fact, the extraction of free data occurs in despite of any kind of reciprocity between the data miners and the miners. There is an enormous distance between the people and their co-creation of intangible capital in terms of sharing collective information technology and communication by the economics agents. There isn't any material reciprocity between them in the production of intangible digital or virtual assets. The logic of accumulation expulse the user, which is the main factor of revenue, from their personal data, characterizing "such assets as "stolen goods" or "contraband" as they were taken, not given…" (S.ZUBOFF, 2017*).*

3. The algorithmic society. Artificial intelligence departs from big data analysis by assessing data, constructing patterns and profiles, making predictions and generalizations and finally by applying the behavior of the person on her decisions. Data, big data and artificial intelligence close a magic circle to make profits from modified human behavior, without any particular effort of transparency, accountability or non-discrimination. Algorithmic decision-making is not neutral. ”Because human beings program predictive algorithms, their biases and values are embedded into the software instructions”. (D.KEATS CITRON,F.PASQUALE, 2014*).*

J.M.Balkin defines the Algorithmic Society as “a society organized around social and economic decision making by algorithms robots, and artificial intelligence agents; who not only make the decisions but, in some cases, also carry them out”. Data is the fuel that fuels the engines, devices and machines used by artificial intelligence. The issue at stake is governance of humans by humans using a particular technology, thus, we cannot segregate Big Data and Internet connection and artificial intelligence from Big Data.

Algorithms are human creations and there is a clear human responsibility for its use to influence other people. The human creator and inventor of the algorithm programs with data collection addressed to perform particular tasks. Programs are not capable of acquiring information and knowledge or to carry out any other purpose. Programs don’t take actions neither do things with our data. The author is a human being and therefore the author is responsible for the errors, any collateral damage and failures.

With the algorithm occurs something similar to financial derivatives before the financial crisis of 2008. During that time, *Bernard Buffet warned* against their potential power of destruction, which was later confirmed. The problem is not the algorithm, but the humans which create and use them as weapon of mass destruction.

The dark side of Big Data is very dangerous and it can damage lives at very critical moments, i.e. when going to college, borrowing money, getting

sentenced to jail or finding and holding a job. All of these life domains are increasingly controlled by secret models wielding arbitrary punishments."(CATHY O`NEIL, 2016*)*

Deregulation is the kingdom of the algorithm. If this situation doesn't evolve in a different direction, there will be a growing instrument of privacy vulnerability and perpetuation of social inequalities. Besides, there is a clear risk of systemic crisis, because the unknown begins to prevail over the known predictions and performances. It seems that we are just on the edge. The digital arrogance applied without care could be the source of troubling dynamics, something similar to environmental pollution. The negative externalities will be superior to the positive ones until the explosion of the systemic crisis.

4. Algorithmic principles. *J.M.Balkin* proposes three principles on artificial intelligence.

A) Information Fiduciaries.

The first principle is that those who use robots, artificial intelligence agents and algorithms have duties of good faith and trust toward their end users and clients. The basic duty of the *information fiduciaries* is that they are not permitted to induce trust in their end users and then turn around and use the information they collect in ways that betray that trust. There is an asymmetry between the Big Data agents and you, because they know a lot about you and you don't know a lot about them.

The principle relies on good faith, non-manipulation, and non-domination as obligations for information fiduciaries (*Google, Facebook, Twitter, and Apple).* Mistrust should not be a priority for artificial intelligence players, on the contrary, it is trust that builds relationships. For this reason, this principle has a broad breath as a collective and social meaning purpose, susceptible of inspiring regulation, sanctions or law.

B) Algorithmic operators have public duties toward general public.

The use of algorithms can harm not only the end user or the client, but many more. The motivation is that the public interference on business is morally justified when it is needed to prevent real or potential damages. Damage to others entails frustration, obstruction or defeat of an interest, all kind of things that improve o worsen our welfare. This principle is connected, as we will see, with the precautionary principle.

C) **The central public duty of algorithmic operators is not to be algorithmic nuisances. They may not externalize the social costs of their use of algorithms onto the general public.**

The principle deals with the negligent use of computational capacities that externalizes costs onto innocent others, or, a nuisance. The concept is related to the externalities produced by the environmental pollution. The companies must adopt methods that are justify from the standpoint of society as a whole.
J.M.Balkin mentions harms to reputation, by classification or risk assessment; discrimination; normalization or regimentation; manipulation; lack of due process, transparency and interpretability.

"We might sum up this discussion by saying that algorithms (a) construct identity and reputation through (b) classification and risk assessment, creating the opportunity for (c) discrimination, normalization and manipulation, without (d) adequate transparency, monitoring, or due process.

The *Balkin* principles are important because they define the algorithmic risks around three main criteria: (i) precautionary duty, (ii) responsibility failure of the economic operators and (iii) disclosure of the secrecy about the means and purposes fulfilled by the artificial intelligence or "arbitrariness by algorithm". Although algorithmic predictions are capable of harming individuals when they have opportunities in life often in arbitrary and discriminatory ways, they remain secret". (D.KEATS CITRON & FRANK PASQUALE, 2014).

The new technology brings progress but also high risks and harm to others. There is an obligation to translate in values, principles and rules the behavior of economic operators when it is morally problematic.

The above is a good point of departure because it excludes some of the more dangerous misconceptions and misunderstandings on the matter, for example, the homunculus fallacy or the android fallacy. Artificial intelligence is human intelligence and therefore it must be subject to protection of personal rights, precautionary clauses and responsibility failures.

5. About the governance common principles. Each community has its own moral values which inform the social dimension and supply criteria for the rules. There are not any rules without a moral dimension. These principles can be described as superior common standards. The importance is that the common principles transpose the human values of fairness and justice and the direction, the general directive or trend, which drive the lawmaker and the law.

-**Privacy protection and civil liberties.**

"Knowledge is power. To scrutinize others while avoiding scrutiny one is one of the most important forms of power. Firms seek out intimate details of potential consumers and employees' lives, but give regulators as little information as they possible can about their own statistics and procedures…The decline in personal privacy might be worthwhile if it were matched by comparable levels of transparency from corporations and governments. But for the most part it is not."(F.PASQUALE, 2015).

The algorithmic decision making increases interference in everyday lives under a logic essentially opaque. The automated predictions, generalizations, patterns, are secret and make impossible challenge the decision, preventing the reaction against probable discrimination on employment, credit scores, insurance risk or, even, in law enforcement, sentencing.

The question is whether it is possible to have the advantages of the new information technology without sacrificing privacy and as *D.J. Solove* points out:"The protection of privacy in the information age is a question of social design".

The balance for now is against individual rights and personal liberties. Damages are extended and simultaneous, in collection, processing, dissemination, and invasion of information. Our identity "is built by others" and it is reused and converted in distortion by appropriation of the new identity.

"I classify as a privacy violation a problem I call *distortion*, which involves disseminating false or misleading information about a person."*(*D.J.SOLOVE, 2008*)* The main issue is the invasion on the decisions that a person can make. Distortion triggers invasion, caused by secret software programs through algorithms predictions. There is no neutral data nor neutral algorithms, sensitive information – gender, age, social status, religion, race, is the foundation for the predictions.

That means that caution and care on data mining and the algorithmic process is needed, because there should be a clear alignment with the person dignity in face of automated decisions. It is not only a problem of data protection, but also of human rights.

-Internalization of externalities.

The *algorithmic nuisance* (J.M.BALKIN, 2017*)* has the same sense of the *pigouvian* externalities.This is a well-known concept in environmental science.There are activities which don't reflect the real social costs of a resource use; so economic agents should have been forced to internalize them.In other cases, the social costs goes beyond the participants, on others,unrelated to the activity.The algorithmic nuisance harms others through the responsibility failure affecting reputation; disparate treatment and impact;generalization;manipulation;opacity.At a minimu, setting an identity which is artificial and different to the true human being identity.

Internalization opens the way to the precautionaire principle:when an activity raises threats of harm to human health, safety, or the environment, precautionairy measures should be taken even if some cause-and effect relationships are not scientifically and fully proved.There is no obligation to wait to the final scientific solution to prevent risks and harms, because that could be too late for the general prevention.There are founded suspicions on the effects of the algorithm society which incite to adopt regulations based in the beliefs or premonitions about its future consequences, without scientific certainty, at the moment. The scientific uncertainty shouldn`t be an excuse to the adoption of measures preventing the possibility of the worse-case scenarios.

Taxation could be a tool to balance the difference between social and private costs induced by the internalization of the agent`s undesiderable behavior.There is here an original idea of a tax on collection,storage,treatment and sale of data due to *Collin-Colin.*

- Bit property. Artificial intelligence ought to be property.

The artificial intelligence "are artifacts: they are product of human labor…From the normative and empirical premises, it would seem to follow that the makers of AIs are entitle to own them."(L.SOLUM, 1992*).*

The first corollary is thay always there is an owner,programmer, controller,who has the property or commands the algorithm.So the responsibility might always be attributable, if that is the issue, to a human being.The liability for harm caused by ALs belong to their owners.

The second corollary is that artificial intelligence artifacts must be qualified as intangibles assets, included the robots, oriented for profits or military and security purposes, as information or ,more, as surveillance assets(*Zuboff).*The definition will secure the fair accountancy and taxation rules of surveillance or information intangibles.

Bit property accentuates the equivalence between property and information assets, that must be organized in broad terms as an open protocol of communication,information and data storage .Property is a procedure rather

than a set of defined attributes.Property is a procedure to communicate information regarding and identity to a resource. The flow of information moves like “waves in a lake, from their place of origin” (J.FAIRFIELD, 2015*).*

The bit property seems accurate to assess if artificial intelligence property is secure and safe, susceptible to human control and aligned with human interests.In other words,it is the foundation to establish a public certification system in a neutral environment, to determine full ,partial or inexistent liability for designers, programmers,manufacturers.Besides, will be possible to establish rules for precertification research and testing of artificial intelligence.”At some point,the legal system will have to decide what to do when those machines cause harm and whether direct regulation would be a desiderable way to reduce such harm.”*(*M.U.SCHERER, 2016).

There is a huge legal challenge for the public,private, commercial,accountancy, employment and taxation ,local and international rules. Artificial intelligence is an **unknown unknown**, forming part of ”the ones we don`t know we don`t know” (E.HEMINGWAY*).*

We need national and international rules to define the level playing field of artificial intelligence between the organizations for profit and public entities who create the algorithms and those who are governed by them. This means an internationally legally binding instrument, through the United Nations *International Telecommunication Union* or, through *soft law*, as Recommendations, Guidelines, Standards, Good Practices and national laws and policies as partial contributions previously to a general regulation. The question it is under which principles and standards.

References

M. MINSKY**,** Semantic Information Processing,M.Minsky ed.,MIT Press,1969.
S.ZUBOFF**,** Big Other:surveillance capitalism and the prospects of an information civilization,Journal of Information Technology, 2015,30.
L.M.LUPOCKI**,** Algorithmic Entities, 95 Washington University Law Review,ssrn.com/abstract=2954173
P.DOMINGOS**,** A Few Useful Things to Know About Machine Learning,Department of Computer Science and Engineering,University of Washington, 2013.

L.BARRET, Deconstructing Data Mining:Protection Privacy and Civil Liberties in Automated Decision-Making,Geo.L.Tech Rev. 1253, 2016.
J.KAPLAN, Artificial Intelligence,Oxford University Press, 2016.
M.R.CALO, Robots and Privacy,2010, ssrn.com/abstract=1599189
V.MAYER-SCHONBERGER,K.CUKIER, Big Data, Garzanti, 2013.
D.J.SOLOVE, "I' ve Got Nothing to Hide" and Other Misunderstandings of Privacy, 2008, ssrn.com/abstract=998565; The Digital Person,2004 New York University.
S.RODOTA**,** Internet ha bisogno di nuove regole, La Reppubblica, 27-11-2014.
J.M.BALKIN**,** The Three Laws of Robotics in the Age of Bid Data, 78 Ohio St. L.J.,2017.
Y.MOULIER BOUTANG, Vers un capitalism cognitive, Paris, 2001, A.Corsani, P.Dieuaide, C.Azais.
P.COLLIN-N.COLIN**,** Mission d' expertise sur la fiscalitè de l' economie numerique,janvier, 2013, Paris.
J.LANIER, Who owns the future?, 2013,New York.
CATHY O`NEIL*,* Weapons of Math Destruction:How Big Data Increases Inequality and Threatens Democracy, Crown, 2016.
D.KEATS CITRON & FRANK PASQUALE, The Scored Society:Due Process for Automated Predictions,Washington Law Review, 2014,89:1
F.PASQUALE, The Black Box Society,The Secret Algorithms That Control Money and Information,Harvard University Press, 2015.
L.SOLUM, Legal Personhood for Artificial Intelligence, North Carolina Law Review, 1992.
J.FAIRFIELD, "BitProperty",Washington and Lee University School of Law,2014-17,October 2014,California Law Review, 2015.
M.SCHERER**,** Regulating Artificial Intelligence Systems:Risks,Challenges,Competencies,and Strategies,Harvard Journal of Law & Technology,29,2, 2016.

La protezione dei dati personali al tempo degli algoritmi intelligenti e dei robot umanoidi

di **RICCARDO PISELLI**

Abstract

This paper addresses the mutual interrelations between the new right to privacy and the latest applications of Artificial Intelligence (AI) and robotics. On the one hand, being personal data the essential resource for the digital economy, AI and robots raises multiples privacy concerns in terms of direct surveillance and private spaces' intrusions. On the other, following the enactment of the General Data Protection Reform, the emergence of new privacy rights and the functional shift of the right to privacy are predicted to have disruptive consequences on the innovation in the field of AI and robotics. Rights such as the right to cancellation and the right to data portability question the economic nature of data as commodities. An unprecedented blending of disciplines emerge in that area with regard of machine learning and deep learning algorithms, which use data as the raw material of knowledge.

1. Premessa. «È il fatto di essere visto incessantemente, di poter sempre essere visto, che mantiene in soggezione l'individuo disciplinare» scrive Michel Foucault in *Sorvegliare e punire*: nella prigione perfetta il sorvegliato non sa mai esattamente quando è sorvegliato e la cosiddetta "veduta diseguale" lo conduce ad un'autodisciplina inesorabile, o a quello che Foucault chiama il "corpo docile". E' la stessa teoria al cuore del *panoptismo* ideato da Jeremy Bentham. Ma siamo davvero sicuri che questi meccanismi valgano solo nella particolarità della detenzione?

Non è forse attraverso questi stessi parametri che dobbiamo cominciare oggi a misurare anche la nostra libertà, includendo la coscienza di ciò che di noi è perennemente controllato da altri anche a nostra insaputa?

La strepitosa estensione della tecnologia a disposizione del Grande Fratello impone un veloce e radicale ribaltamento di tutte le prospettive.

Ecco allora che Intelligenza artificiale e diritto alla privacy appaiono improvvisamente tra loro legati sotto diversi profili.

Da un lato, le più recenti applicazioni della Intelligenza artificiale, facilitando l'acquisizione d'informazioni personali, moltiplicano le potenziali intrusioni nella sfera di riservatezza di ciascuno. Tale dialettica conflittuale, invero, non è nuova ed ha caratterizzato anche i rapporti tra più classiche tecnologie dell'informazione e diritto alla riservatezza (CHEMERINSKY 2007; GAVISON 1980).

Dall'altro lato, specularmente, la moderna evoluzione del diritto alla *privacy* introduce nuovi limiti allo sviluppo e alla diffusione dell'Intelligenza artificiale.

Il presente lavoro intende esplorare tale tensione alla luce delle ultime innovazioni tecnologiche e dell'imminente recepimento della General Data Protection Reform.

2. L'intelligenza artificiale. Algoritmo, informazione e memoria. Nella storia delle civiltà nulla sembra avere maggiormente affascinato l'uomo quanto l'evoluzione della conoscenza, lo studio dei meccanismi della mente: dalla maieutica socratica ai sistemi aristotelici, dall'episteme neoplatonica al dualismo cartesiano, dalla sostanza di Spinoza all'innatismo di Leibniz fino alla sintesi di Kant fra ragion pura e ragion pratica, dal sistema logico-ontoloigico di Hegel fino alle moderne teorie cognitive.

La storia dell'Intelligenza Artificiale (da ora I.A.) può essere scandita in tre fasi. La prima vede lo sviluppo di sistemi intelligenti nell'ambito della computazione. La seconda è caratterizzata dall'imitazione dei processi di soluzione di problemi e dei ragionamenti umani. La terza, infine, si

contraddistingue per la creazione di sistemi "esperti" e modelli cc.dd. "connessionisti (WARWICK 2012).

Più recentemente, con la progressiva attenzione prestata da legislatori e *policymakers* al fenomeno dell'industria 4.0, si inizia a parlare di I.A. anche al di fuori dei laboratori in cui essa per lungo tempo era stata confinata. Essa entra così silenziosamente, quasi inavvertita, nella vita quotidiana delle persone, fino a plasmare, addomesticare e spesso ottundere le loro menti, nella totale assenza di autocoscienza e di regolazione giuridica.

Occorre, innanzitutto, una dovuta precisazione. La I.A. *in senso lato* costituisce un cerchio al cui interno possono essere incluse numerose applicazioni (RUSSEL 2009). Si pensi, su tutte, alla branca della cibernetica o a quella della robotica, che costituisce una sotto-branca della prima e si occupa di quegli algoritmi intelligenti che operano in un ambiente esterno. Ogni approccio al tema, pertanto, non deve cadere nell'errore di confondere una parte con il tutto.

La I.A. *in senso stretto* si compone di tre elementi: uno proprio della macchina, uno a essa esterno e, per finire, uno indifferentemente interno o esterno alla macchina. Essi sono l'*algoritmo*, l'*informazione* e la *memoria*.

Ciò è vero con riferimento a ogni tipo di applicazione intelligente e trova riscontro nelle definizioni più diffuse di I.A., che tuttavia non prendono sempre in considerazione tutti e tre gli elementi[1].

1 Si veda Relazione del Parlamento europeo, recante *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, doc. A8-0005/2017, 27 gennaio 2017, p. 22, che tuttavia si occupa limitatamente solo di 'robot intelligenti', secondo cui: "È opportuno stabilire una definizione comune europea di robot autonomo intelligente, comprese eventualmente le definizioni delle sue sottocategorie, tenendo conto delle seguenti caratteristiche: – la capacità di acquisire autonomia grazie a sensori e/o mediante lo scambio di dati con il proprio ambiente (interconnettività) e l'analisi di tali dati – la capacità di apprendimento attraverso l'esperienza e l'interazione – la forma del supporto fisico del robot – la capacità di adeguare il suo comportamento e le sue azioni all'ambiente". Si veda, anche, Executive Office of the President, National Science and Technology Council Committee on Technology, *Preparing for the future of Artificial Intelligence*, October 2016, p. 6, dove viene evidenziato che: "There is no single definition of AI that is universally accepted by practitioners. Some define AI loosely as a computerized system that exhibits behavior that is commonly thought of as requiring intelligence. Others define AI as a system capable of rationally solving complex problems or taking appropriate actions to achieve its goals in whatever real world circumstances it encounters". Vedi anche il recente *discussion paper* dell'Information Commissioner's Office del Governo britannico, *Big Data, artificial intelligence, machine learning*

Infatti, da un punto di vista empirico, l'I.A. è il prodotto di un *algoritmo* in grado di processare e sintetizzare una certa quantità di dati in un tempo inversamente proporzionale alla potenza di calcolo della macchina stessa. Ogni algoritmo di I.A. è poi concepito per svolgere una determinata *funzione*, per raggiungere un certo *output* prestabilito dal programmatore.

Tuttavia, l'algoritmo – *rectius* la stringa di linguaggio che compone l'algoritmo – costituisce solo una componente, forse quella più importante, della I.A.. La seconda componente è data dalla informazione processata. Inutile dire, infatti, che maggiore è la mole dell'informazione processata, più raffinata e, si potrebbe dire, 'intelligente', sarà la risposta che la macchina darà a uno specifico stimolo esterno. Quindi, la soluzione data da una macchina intelligente a un certo problema sarà, in termini probabilistici, tanto più esatta quanto maggiore è l'informazione sulla cui base tale soluzione viene fondata.

Infine, il terzo elemento è dato dalla memoria, che consente l'immagazzinamento d'informazioni. Tale elemento non deve essere sottovalutato nell'analisi del fenomeno, giacché maggiore è l'informazione da processare, maggiore sarà lo spazio fisico o virtuale da impegnare.

L'algoritmo, sotto un profilo giuridico, costituisce un'invenzione, un'opera dell'ingegno e, come tale, assoggettabile alla tutela intellettuale come *intangible asset*. Sul punto, la scienza giuridica, pur nella divergenza di vedute circa il tipo di tutela da accordare al software, sembra essere concorde.

L'informazione in senso ampio, invece, appare difficilmente inquadrabile nell'ambito di una sola definizione giuridica. Ciò è dovuto alla natura composita di un termine che racchiude dati, pubblici o privati (talvolta anche personali o sensibili), fatti e interazioni bilaterali o plurilaterali. Peraltro, è stato sottolineato come il concetto di informazione non vada confuso con quello di dati. I dati di per sé sono privi di significato: lo assumono solo in quanto processati dall'algoritmo (ESPOSITO 2017, BATESON 1972).

---

and data protection, 1 marzo 2017; Government Office for Science, *Artificial intelligence: opportunities and implications for the future of decision making*, 9 November 2016, secondo cui per Intelligenza Artificiale (I.A.) s'intende "the analysis of data to model some aspects of the world. Inferences from these models are then used to predict and anticipate possible future events".

Per finire, la memoria costituisce né più né meno che un magazzino, un luogo dove registrare informazioni. Un luogo che, come ogni spazio (fisico o virtuale), si presta a essere illegalmente violato o alterato. Tale circostanza si salda alle problematiche tradizionali che il nascente filone di studi in materia di *cyber security* sta impegnando da qualche anno ormai la dottrina più attenta.

Quando la macchina intelligente è dotata di un substrato fisico, che le consente di muoversi e interagire col mondo esterno, un ulteriore elemento si aggiunge ai tre che compongono l'intelligenza artificiale. Tale ulteriore elemento è il *corpo* della macchina, che, nelle sue quattro componenti, viene così definita *robot*. Il corpo della macchina, rileva sotto un profilo giuridico, su due piani: da un lato, esso estende gli effetti delle azioni della macchina nel mondo esterno; dall'altro, essa consente l'interazione della macchina con l'uomo e con la realtà fenomenica e soprattutto, in forza di questa interazione, laddove l'algoritmo sia così programmato, *l'apprendimento.*

Sotto questo ultimo profilo, deve darsi conto, peraltro, della tendenza attuale della filosofia della scienza ad ampliare la ricerca verso la c.d. E.A. (l'Empatia Artificiale), ossia quell'area della ricerca robotica impegnata nella costruzione di agenti sintetici dotati di competenze affettive (DUMOUCHEL 2016).

3. L'impatto delle più recenti applicazioni di I.A. sulla *privacy*. Verso un perenne stato di sorveglianza. L'I.A. e le sue molteplici applicazioni incidono sulla *privacy* delle persone in maniera molto più pervasiva rispetto alle precedenti innovazioni tecnologiche. Da un lato, infatti, i più recenti sviluppi compiuti in materia di I.A. hanno facilitato le modalità di acquisizione dei dati e, per l'effetto, la quantità di dati disponibili. Dall'altro, le ultime innovazioni in materia di *data mining*, hanno agevolato la capacità di estrarre dalle informazioni *pattern* rilevanti, incidendo sull'elemento qualitativo dell'informazione.

Quanto al primo profilo, paradigmatica è la progressiva diffusione commerciale di robot, androidi, cyborg e droni intelligenti. Non più confinati al solo settore dell'automazione industriale, i robot oggi sono impiegati per

svolgere le più disparate funzioni: dal trasporto di merci alla ricognizione di territori inospitali, dall'assistenza domestica, alle applicazioni militari, dagli interventi chirurgici, all'assistenza sanitaria. A livello mediatico, grande attenzione è stata prestata alle note *Google cars*, le auto senza guidatore di Google, e ai problemi di regolazione a essi collegati. A livello europeo, proprio la necessità di adattare le norme sulla responsabilità civile alla nuova generazione di robot, dotati di capacità di adattamento e apprendimento, ha condotto all'approvazione della nota risoluzione del Parlamento europeo recante *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*[2].

Per ciò che qui interessa, il progressivo sviluppo della robotica incide sulla privacy, in quanto i robot rendono possibile l'acquisizione materiale di informazioni ulteriori non altrimenti acquisibili con altri mezzi. Difatti, i robot possono raggiungere luoghi inaccessibili all'uomo e sono equipaggiati con sensori e telecamere in grado di registrare tutto ciò che avviene in un dato ambiente. Ryan Calo, a tal proposito, sottolinea come i robot incidano sulla privacy delle persone in tre diversi modi (CALO 2012). In primo luogo, essi consentono la diretta sorveglianza di determinati soggetti (SINGER 2009). In secondo luogo, i robot soprattutto quelli domestici, forniscono delle finestre da cui osservare spazi privati e non accessibili (ZITTRAIN 2008). E infine, lo sviluppo di robot dalle parvenze umane e capaci di interagire a livello sociale con l'uomo potrebbe condurre a più intrusive e sottili invasioni della sfera privata.

In relazione a quest'ultimo punto, infatti, Calo sostiene che una delle funzioni della privacy più diffusa nella letteratura prevalente (WESTIN 1967) sia quella di difendere momenti di intimità, riflessione e finanche solitudine. In questo senso, la sempre maggiore diffusione di robot dalle funzioni più sociali in ambienti domestici rischia di azzerare tali momenti, confermando l'affermazione di H.R. Ekbia secondo cui "computers are everywhere" (EKBIA 2008). A ciò si aggiunge che le sembianze umanoidi di un robot hanno effetto sul modo in cui

2 Relazione del Parlamento europeo, recante *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, doc. A8-0005/2017, 27 gennaio 2017.

le persone fisiche interagiscono nella realtà, sentendosi costantemente sotto giudizio e vivendo in uno stato di perenne eccitazione (CALO 2010; SPROUL 1996).

Ma non occorre correre con l'immaginazione ai robot umanoidi per rendersi conto di come la tecnologia faciliti l'acquisizione di informazioni ulteriori e rilevanti, moltiplicando i rischi per la privacy. Numerosi *devices* indossabili, braccialetti elettronici integrati con scarpe da corsa e applicazioni del nostro *smartphone* consentono il tracciamento delle funzioni biologiche della persona e l'incameramento di una elevata mole di dati sensibili. Sotto il vessillo della semplificazione nell'offerta di servizi, vengono giornalmente raccolti infinite quantità di dati biometrici, che consentono di schedare gli individui, concretizzando quell'immaginario di mondo preconizzato da Latour, caratterizzato da "fragments of intelligence distributed through machines, fragments of machines dispersed through bodies, fragments of organizations morphed into software lines, fragment of codes sticking into institutions, fragments of subjects floating into virtual space" (LATOUR 1995).

Quanto al secondo profilo, occorre far riferimento alle più evolute tecniche di *data mining* e ai recenti algoritmi di *machine learning*[3] e *deep learning*[4]. Questi pongono nuovi e rilevanti problemi per la privacy. Infatti, l'implementazione del *data mining* permette di estrarre informazione da metadati presenti in rete, evidenziando correlazioni e differenze non identificabili dall'uomo ed estraendo informazioni rilevanti da informazioni

3 Il c.d. apprendimento automatico (*machine learning*) viene definito dall'Information Commissioner Office come "the set of techniques and tools that allow computers to think by creating mathematical algorithms based on accumulated data". Si veda, ICO, *Big Data, artificial intelligence, machine learning and data protection*, 1 marzo 2017. Si veda anche Executive Office of the President, National Science and Technology Council Committee on Technology, *Preparing for the future of Artificial Intelligence*, ottobre 2016, che lo definisce come "statistical process that starts with a body of data and tries to derive a rule or procedure that explains the data or can predict future data".

4 Il c.d. deep learning "involves feeding vast quantities of data through non-linear neural networks that classify the data based on the outputs from each successive layer". Si veda, Information Commissioner Office, *doc. cit*.. In senso analogo si esprime l'Executive Office of the President, National Science and Technology Council Committee on Technology, *doc.cit*., secondo cui "Deep learning uses structures loosely inspired by the human brain, consisting of a set of units (or "neurons"). Each unit combines a set of input values to produce an output value, which in turn is passed on to other neurons downstream".

secondarie. Cosi, ad esempio, è stato dimostrato che i vegetariani perdono meno aerei rispetto al resto della popolazione (MAYER-SCHÖNBERGER 2013) o che il tasso di divorzi in Maine è legato all'uso pro capite di margarina[5]. E, in questo senso, la privacy potrebbe essere minacciata dalla non corrispondenza al vero di tali correlazioni.

L'apprendimento automatico, e in particolare il *deep learning*, fondato sulla tecnologia delle reti neurali al fine di replicare il funzionamento del cervello umano, adduce poi un ulteriore grave problema per la privacy. Infatti, gli algoritmi di *machine learning* sono in grado di compiere generalizzazioni a partire da esempi, al fine di svolgere una data funzione. Tuttavia, l'informazione processata diviene parte dell'algoritmo stesso, andando a formare un ulteriore *layer* della rete neurale, che a sua volta processerà ulteriori dati. Ecco, dunque, che tali algoritmi non solo processano dati, ma evolvono con l'esperienza (i.e. con la memorizzazione dell'informazione prima processata). Ed ecco che i dati, non costituiscono più e soltanto materiale grezzo da processare, ma guidano l'apprendimento futuro. Tale "appropriazione" del dato processato, conseguentemente è rilevante per il diritto della privacy.

4. Da "*right to be let alone*" a strumento di regolazione. L'impatto del moderno diritto alla *privacy* sui futuri sviluppi della I.A. La prima elaborazione del diritto alla privacy si deve a Louis D. Bradeis e Samuel D. Warren (WARREN, BRANDEIS 1890), che nel breve saggio intitolato *The Right to Privacy* e pubblicato nell'Harvard Law Journal nel 1890 ne diedero un'accezione negativa quale *right to be let alone*, quale diritto dell'uomo a essere lasciato solo, quale possibilità di scelta di esclusione dal consesso sociale.

Molti anni sono passati da allora e questo particolare significato di privacy ha lasciato il posto a nuove formulazioni normative del suddetto diritto, quale diritto di mantenere il controllo sulle proprie informazioni e,

5 http://www.tylervigen.com/spurious-correlations

conseguentemente, come diritto all'autodeterminazione informativa (RODOTÀ 1991).

Tale passaggio da una connotazione negativa del diritto alla privacy – intesa quale non ingerenza nella sfera privata – a una connotazione positiva – come autodeterminazione e controllo - è coincisa con l'avvento computer (WESTIN 1970) e si ritrova nelle prime formulazioni normative del diritto alla privacy.

Sul solco di questa evoluzione si inserisce la c.d. General Data Protection Reform[6], che in un certo senso costituisce una risposta all'aumento esponenziale dei *big data* e ai progressi tecnologici avvenuti in materia di *data mining*, I.A. e robotica. Esso, in questo senso, introduce nuovi principi e disposizioni volti a potenziare le garanzie di un controllo effettivo delle persone sui propri dati personali.

Il controllo viene assicurato da penetranti obblighi posti in capo a chiunque proceda al trattamento dei suddetti dati[7] e da severe sanzioni in caso di inosservanza degli stessi obblighi[8]. Al contempo, al controllo viene affiancato il riconoscimento normativo della "piena disponibilità" dei propri dati personali in uno con la presa di coscienza del loro valore economico. Diritti come quello di rettifica (art. 16), quello alla cancellazione dei dati (art. 17), quello di limitazione di trattamento (art. 18) o quello alla portabilità dei dati (art. 20) delineano un rinnovato diritto alla protezione dei dati personali che poggia su un sostanziale *empowerment* del consumatore rispetto a tutti quegli operatori il cui modello di business poggia sul trattamento di dati personali.

La privacy, da questa prospettiva, diviene lo strumento di una regolamentazione economica, sovrapponendosi alla disciplina della concorrenza[9].

6 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati.
7 Cfr. Capo IV.
8 Cfr. Capo VIII.
9 Basti pensare a tal riguardo al diritto alla portabilità dei dati (art. 20), cui è sottesa, secondo il Garante della Privacy, "L'aspettativa…che, oltre ad ampliare il margine di controllo dei consumatori impedendo forme di 'lock in' tecnologico…promuova l'innovazione e la

Non è infatti un caso che, poco più di un anno fa, le autorità della concorrenza francese e tedesca abbiano formalmente adottato un documento di studio congiunto sugli effetti anticoncorrenziali derivanti dalla raccolta, dal trattamento e dall'utilizzazione dei dati[10].

In questo senso, da baluardo contro l'altrui intrusione nella sfera privata, la privacy diviene dapprima diritto alla libera autodeterminazione della persona e all'autenticità e veridicità dell'informazione, per trasformarsi in strumento di regolazione economica.

In quanto tale, la protezione dei dati personali nella sua moderna accezione, entra in scelte di politica economica e pone innumerevoli implicazioni in relazione all'innovazione tecnologica. Ciò è di particolare evidenza nel caso della I.A..

Volgendo, infatti, l'attenzione ai più moderni algoritmi di *machine learning* e *deep learning*, ci si accorgerà di come questi abbisognino di grandi quantità di dati per funzionare. Si pensi, ad esempio, all'algoritmo usato da Uber per prevedere in modo accurato le abitudini di viaggio degli utenti o categorie di utenti o all'algoritmo di Amazon che offre esperienze di acquisto sempre più personalizzate per l'utente. Si pensi agli algoritmi di riconoscimento vocale e agli assistenti virtuali degli *smartphones* o GPS e agli algoritmi utilizzati dai maggiori motori di ricerca. Ma si pensi ancora alla piattaforma Watson Health, che analizza milioni di dati sanitari per addivenire a diagnosi sempre più precise e trattamenti sanitari più efficaci. Tutti questi dati rientrano, infatti, a pieno titolo nella definizione di "dati personali", elaborata dal nuovo regolamento europeo e incentrata sul perno della riconducibilità, diretta o indiretta, dei dati stessi alla persona fisica[11]. Conseguentemente, al loro trattamento dovranno applicarsi tutte le disposizioni del Regolamento (UE) 2016/679.

---

condivisione di dati personali fra titolari del trattamento in piena sicurezza e sotto il controllo dell'interessato". Cfr. Garante della Privacy, gruppo di lavoro articolo 29 in materia di protezione dei dati personali, Linee-guida sul diritto alla "portabilità dei dati", adottate il 13 dicembre 2016.

10 Si veda il Report congiunto della Autorité de la concurrence e della Bundeskartellen, *Competition Law and Data*, 10 maggio, 2016.

11 I "dati personali", nell'ambito del nuovo regolamento UE, sono definiti in senso ampio come "qualsiasi informazione riguardante una persona fisica identificata o identificabile (…) direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un

4.1 La trasparenza sull'uso dei dati in una "*black box society*". La relatività di un concetto. Nel febbraio 2017, il Tribunale Amministrativo Regionale per il Lazio, annullava una nota ministeriale, con la quale il Ministero dell'Istruzione (MIUR) denegava l'accesso all'algoritmo usato per gestire i trasferimenti interprovinciali dei docenti della scuola primaria e d'infanzia. La sentenza, accolta con grande clamore mediatico, costituisce l'atto finale di una vicenda cominciata più di un anno prima, quando diversi insegnanti iniziarono a lamentare inspiegabili trasferimenti presso sedi scolastiche a diversi chilometri distanti dalla propria residenza. Di fronte alla richiesta pervenuta di rendere pubblici i codici sorgente dell'algoritmo stesso, il MIUR rispondeva dapprima fornendo una generica descrizione della procedura informatica seguita e, poi, negando l'accesso richiesto in ragione *inter alia* della tutela del software quale opera dell'ingegno e della non assimilabilità dello stesso a un atto amministrativo. Nel disattendere le suddette argomentazioni, il TAR Lazio finiva per ordinare l'accesso all'incriminato algoritmo dopo averlo qualificato come "atto amministrativo informatico"[12].

La descritta vicenda mette in luce come algoritmi intelligenti dominino la vita di tutti i giorni e prendano decisioni che finiscono per impattare notevolmente sulla sfera dell'individuo: gli algoritmi sollecitano le decisioni di acquisto e i nostri gusti musicali o cinematografici, decidono il percorso più breve per guidarci da un punto A a un punto B, guidano le decisioni d'investimento finanziario e determinano i cambi tra valute reali e finanche criptovalute. Frank Pasquale (PASQUALE 2015), nel mirabile volume intitolato *The Black Box Society*, descrive una società dove l'informazione e la conoscenza, che costituiscono la quintessenza del potere (BALKIN 2008), sono appannaggio di pochi, schermati da *trade secrets* e disponibili solo agli *insiders*.

numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o piu elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (art. 4, comma 1). Si noti, inoltre, che rispetto alla precedente direttiva 95/46/CE, il regolamento aggiunge nel corpo della definizione il riferimento anche a "quei dati relativi all'ubicazione" e a un generico "identificativo online", estendendone oltremodo il perimetro.

12 TAR Lazio, Sede di Roma, sez. III^, 14.2.2017, n. 3769.

Dietro la promessa della tecnologia di predire il futuro attraverso la devoluzione di complessi calcoli statistici a macchine dalla sempre più elevata capacità computazionale, si cela il rischio di una società in cui complesse scelte di policy e valutazioni del rischio sono devolute a processi automatizzati non intellegibili. Sistemi reputazionali e complessi algoritmi di calcolo, guidano la finanza e il commercio globale, sfuggendo all'accesso e alla comprensione dei regolatori e minacciando la privacy, la dignità e la libertà dei singoli. Big data e intelligenza artificiale costituiscono i capisaldi di una siffatta società dove mai il conflitto tra innovazione tecnologica e privacy è stato più netto.

A tal riguardo, il nuovo regolamento europeo, come si è avuto modo di accennare, introduce disposizioni che cercano di rendere più trasparente il trattamento dei dati attraverso algoritmi di I.A.. Questi, infatti, siano essi ascrivibili a modelli di intelligenza artificiale debole o forte, processano dati, che rientrano a pieno titolo nella nozione di "dati personali" fornita dal nuovo regolamento. Ecco, dunque, che il "trattamento" che di tali dati viene fatto attraverso l'algoritmo diviene rilevante per il moderno diritto della privacy, configurando una specifica fattispecie di "trattamento automatizzato".

All'articolo 1, il regolamento europeo annovera tra i principi applicabili al trattamento dei dati "la liceità, correttezza e *trasparenza*". Alla trasparenza sono poi dedicate due sezioni del capo 1, la prima intitolata "trasparenza e modalità" e la seconda "informazione e accesso ai dati". Più nello specifico, è previsto che il titolare del trattamento adotti misure appropriate per fornire all'interessato tutte le informazioni e comunicazioni "relative al trattamento in forma coincisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro" (art. 12). Le informazioni da fornire riguardano sia quei dati personali che siano raccolti presso l'interessato (art. 13), sia quei dati che siano raccolti altrove (art. 14).

È poi riconosciuto il diritto di accesso dell'interessato, che si sostanzia nel "diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento e, in tal caso, di ottenere l'accesso ai dati personali".

Tale complesso di disposizioni delinea un sistema diretto a dare attuazione alla trasparenza, intesa come intellegibilità e comprensibilità del trattamento. Non a caso, già nel considerando n. 39, si evince che "il principio di trasparenza impone che le informazioni e le comunicazioni…siano facilmente accessibili e *comprensibili*". Eppure, il regolamento, non chiarifica cosa debba intendersi per "comprensibili" e come debba essere interpretato un concetto cosi relativo, destinato a variare da un punto di vista soggettivo e oggettivo. Del tutto intuitivamente, infatti, ciò che è comprensibile a un ingegnere informatico non lo è ugualmente a una casalinga o a un avvocato. E, altrettanto intuitivamente, una cosa è comprendere in astratto le finalità del trattamento, altra cosa è comprendere in che modo tali finalità sono perseguite, ad esempio per sindacarne gli *outputs*. Ancora, una cosa è comprendere che esista un processo di profilazione, altra cosa è comprendere come un profilo sia stato elaborato, nonché "quelle informazioni significative sulla logica utilizzata" (art. 14, comma 2, lett. g)) necessarie per eventualmente sindacarne la corrispondenza al vero.

Come la vicenda dell'incriminato algoritmo del MIUR ha messo in luce, esistono diversi gradi di comprensibilità ma, laddove siano in contestazione le scelte operate da complessi algoritmi di calcolo che intaccano su diritti e libertà dei singoli, questa deve essere assicurata nella forma più ampia possibile, che finisce per coincidere con l'accesso ai codice sorgente dell'algoritmo.

Si giunge qui al nodo del problema, che diventa particolarmente spinoso quando il trattamento dei dati sia svolto per il tramite di algoritmi di I.A. protetti in qualità di opere dell'ingegno o tutelati per il tramite di *trade secrets*. È difatti di tutta evidenza il conflitto latente tra *data protection* e proprietà intellettuale in tutti quei casi in cui complessi algoritmi di calcolo processano dati personali. Tra le limitazioni all'accesso alle suddette informazioni (art. 23), infatti, non figura la necessità di tutelare il segreto industriale e aziendale, eppure, al considerando n. 63, si evince che "(il diritto di accesso) non dovrebbe ledere i diritti e libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti di autore che tutelano il software". Nel silenzio del

legislatore europeo, spetterà probabilmente al neoistituito comitato europeo per la protezione dei dati personali sciogliere il dilemma di quale dei due valori debba prevalere.

4.2. Il *trade-off* tra tutela dei dati personali e libero accesso alla conoscenza. Nel lontano marzo 1991 la Stanford Universiy ospitava il primo simposio mondiale sulle problematiche poste dall'intelligenza artificiale (I.A.) per il diritto della proprietà intellettuale. L'iniziativa ebbe ampia risonanza non soltanto per la presenza di eminenti personalità della Silicon Valley e grandi studiosi della materia, ma soprattutto per il fatto di essere stata organizzata dalla World Intellectual Property Organization (WIPO).

Tra le varie criticità che emersero in quella sede, una in particolare appare cruciale per il presente lavoro. In particolare, Andy Johnson-Laird si chiedeva:

> *"What about the facts used to train the neural network? If they are facts, can they be protected? Well you can say, I have organized them in a particular way, I would like to protect them as a compilation? But the networks learned better when you randomized the facts. How could you protect those? I talk here about the ownership of knowledge, and I know, under the law, ownership and autorship are fairly close together"*[13].

In altri termini, la riflessione che l'ingegnere aveva aperto riguardava proprio la proprietà (c.d. *ownership*) di tutti quei "fatti" utilizzati per affinare la capacità predittiva di un qualsiasi algoritmo intelligente. Infatti, se già al tempo era indubitabile che un algoritmo costituisse un'opera intellettuale, molto più controversa appariva la natura giuridica dell'informazione processata e la possibilità di accordare ad essa una qualsivoglia tutela autoriale. Dalle parole di Johnson-Laird, tuttavia, sembrava chiaro che l'algoritmo da solo fosse una

13 WIPO Worlwide symposium on the Intellectual Property Aspects of Artificial Intelligence, Stanford University (California), United States of America, 25 – 27 marzo, 1991 (ftp://ftp.wipo.int/pub/library/ebooks/wipopublications/wipo_pub_698e.pdf).

semplice scatola vuota (BALKIN, 2017), destinata a essere riempita dall'informazione e che la "conoscenza" fosse la risultante delle due componenti.

Questa relazione simbiotica tra algoritmo e informazione implica due cose: in primo luogo, se l'informazione si compone in massima parte di dati che rientrano nell'accezione di "dati personali", la *data protection* viene a sovrapporsi con la tutela della proprietà intellettuale, nel senso che i dati personali divengono parte integrante dell'originaria stringa di linguaggio di programmazione dell'algoritmo; in secondo luogo, per ciò che qui interessa, se i dati costituiscono la risorsa essenziale per lo sviluppo di algoritmi di I.A., sussiste un *trade-off* tra le opportunità connesse a un libero sfruttamento dei dati e i limiti derivanti dal riconoscimento di un elevato livello di *data protection*, proprio come sussiste un *trade-off* tra libero accesso alla conoscenza e il riconoscimento di diritti di privativa sull'algoritmo. Infatti, in un ecosistema in cui i dati sono il sostrato essenziale della "conoscenza", qualsiasi limitazione al loro accesso, anche se strumentale alla tutela di ulteriori diritti, si traduce in una limitazione della conoscenza stessa, intesa quale bene comune.

4.2.1 Segue. Un insanabile conflitto: la qualificazione dei dati. La sopradescritta dualità conflittuale tra protezione dei dati personali e accesso alla conoscenza trova la sua ragione giustificativa nella diversa qualificazione giuridica che viene attribuita ai dati.

In letteratura è stato rilevato come esistano molteplici definizioni di dati, in relazione a diversi contesti (ZENO ZENCOVICH 2016). I dati, sebbene siano qualificati dalla teoria economica come beni pubblici non rivali e non consumabili (SAMUELSON 1954), sono al contempo *commodities* scambiabili sul mercato.

Con specifico riferimento ai dati personali, poi, il concetto di *commodity*, già in passato, aveva diviso la dottrina prevalente. Da un lato vi erano coloro che consideravano i beni personali veri e propri beni giuridici, di cui l'interessato dispone e che può trasferire mediante la manifestazione del consenso

(MORMILE 2006; MANES 2001; OLIVO 2002). Dall'altro vi erano, invece, coloro che contestavano tale reificazione, sulla scorta del rilievo secondo cui l'interessato, attraverso la manifestazione del consenso al trattamento, non perde il alcun modo la titolarità e il controllo di tali dati (ORESTANO 2003). La *querelle* dottrinale finiva quindi per riguardare la natura del consenso, quale atto negoziale dispositivo di un bene giuridico o, alternativamente, atto meramente autorizzativo di un'invasione nella propria sfera giuridica ad opera di terzi. Nel primo caso, la funzione dispositiva del consenso sarebbe stata tendenzialmente incompatibile con un qualsivoglia atto contrario di revoca, rispondendo all'esigenza di assicurare una certa stabilità al sinallagma contrattuale; nel secondo caso, invece, la revoca sarebbe strumentale ad assicurare la protezione dell'identità personale dell'individuo, rispetto a trattamenti dei dati personali consentiti nel passato.

Siffatta questione è stata risolta dal legislatore europeo, che, a prima vista, sembra aver confermato il secondo indirizzo[14]. Il nuovo regolamento europeo, infatti, nell'attribuire una serie di diritti al titolare dei dati personali oggetto di trattamento, attribuisce all'interessato la facoltà di disporre pienamente dei propri dati, a prescindere dal *consenso* prestato o dal *contratto* sottoscritto con il titolare del trattamento. Tanto è vero che, all'art. 7 comma 3, è stabilito che "L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento (…) Il consenso è revocato con la stessa finalità con cui è accordato". La revoca del consenso, tuttavia ha efficacia solo *pro futuro* e "non pregiudica la liceità del trattamento basata sul consenso prima della revoca".

In ultima analisi, dalla prospettiva del diritto della privacy, i dati personali giammai dovrebbero essere giuridicamente assimilati a una *commodity*. Sembra, dunque, determinarsi un'irreparabile frattura tra la concezione

14 Nello stesso senso di escludere la natura di beni dei dati personali, si è, inoltre, recentemente espresso l'European Data Protection Supervisor (EDPS), opinion 4/2017, 14 marzo 2017, secondo cui occorrerebbe evitare l'uso del termine "*data as a counter-performance*", in quanto "There might well be a market for personal data, just like there is, tragically a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation".

economica dei dati personali e quella giuridica fatta propria dal microcosmo legislativo della *data protection*.

4.2.2 Segue. La rimozione dei dati usati per allenare l'algoritmo, tra diritto alla cancellazione e *machine learning*. È in questo scenario che occorre contestualizzare le implicazioni del nuovo regolamento europeo sui futuri sviluppi delle applicazioni di I.A.. Tra di esse, sembra centrale affrontare quello che parrebbe il punto di emersione di questo inconciliabile conflitto tra le suddette opposte concezioni, vale a dire il rapporto tra algoritmi di *machine learning* e diritto alla cancellazione, anche detto "diritto all'oblio".

Quest'ultimo, portato alla ribalta mediatica dal famoso caso *Google Spain*[15], viene inteso, nella positivizzazione operata dal legislatore europeo, come quel "diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo". Le basi filosofiche del diritto all'oblio affondano nel pensiero di Heiddeger e Ricoeur: il rapporto col passato, particolarmente in Ricoeur, si fonda su una relazione attiva, che permette una rielaborazione del senso proprio di vicende già verificatesi. Se una certa dose di dimenticanza è quasi necessaria per portare a compimento il processo di rielaborazione del passato individuale, ciò non vuol dire che il soggetto debba cancellare le tracce dei fatti accaduti. Potrà, invece, attribuire loro un nuovo significato che sarà condivisibile con la comunità. In questo senso l'identità personale implica necessariamente il confronto con la comunità nel momento in cui essa accede e conosce quel passato. Il potere di ricostruzione del passato del singolo deve saper coesistere con quello che gli altri hanno di poter accedere alle informazioni tipiche di un passato condiviso, di un sapere comune.

Del c.d. diritto all'oblio comunque sono state date diverse e talvolta contrastanti interpretazioni, come "right not to disseminate" (PIZZETTI 2013), ossia diritto alla non divulgazione dei propri dati, come "right to contextualise"

15 Corte di Giustizia UE, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos*, causa C-131/12.

(PIZZETTI 2013), vale a dire diritto alla contestualizzazione dei dati nel tempo e come "right to reinvention" (SOLOVE 2011), come diritto cioè a reinventare il presente disancorandolo dal passato. Tutte le suddette definizioni sono accumunate da un'interpretazione del diritto all'oblio quale diritto funzionale alla costruzione e allo svolgimento della propria identità personale, in una dialettica che vede compartecipe anche l'"altro", appunto il contesto sociale dal quale è impossibile prescindere.

All'opposto estremo, in una relazione conflittuale, stanno invece gli algoritmi di *machine learning*, programmati per sintetizzare attraverso complessi calcoli statistici i dati a disposizione e memorizzarne gli *output* essenziali. In questo senso, l'algoritmo processa una quantità di dati di gran lunga superiore rispetto a quella di cui è a conoscenza il singolo. Esso evidenzia correlazioni e differenze tra metadati ed è in grado di estrarre informazioni rilevanti da informazioni secondarie.

La memoria consente l'apprendimento, che nei casi di apprendimento senza rinforzo, è al di fuori del dominio del programmatore. I dati vengono acquisiti, raffinati, memorizzati e utilizzati come mattoni per costruire, attraverso la loro aggregazione in *cluster* uniformi, l'intelligenza stessa dell'algoritmo. Pur se inaccessibili attraverso l'indicizzazione dei motori di ricerca i dati continuano, dunque, a esistere all'interno di una onnipresente "memoria algoritmica" (ESPOSITO 2017)[16].

Si assiste, in altri termini, a un processo di "appropriazione" e "rielaborazione" dell'informazione da parte della macchina, divenendo l'informazione componente essenziale dell'algoritmo stesso. La relazione che si istaura tra dati e algoritmo è biridezionale. Da un lato, l'algoritmo processa e interpreta i dati che compongono l'informazione, dall'altro, l'informazione fa evolvere l'algoritmo, diventando essa stessa componente dell'algoritmo.

La moderna *data protection*, tuttavia, sembra non prendere direttamente in considerazione questo rapporto nella sua totalità, fermandosi alla disciplina

16 Altri autori hanno affermato che l'algoritmo usa "data exhaust" o "data shadows", generati indirettamente dagli individui sul web (KOOPS 2011).

della “raccolta” e del “trattamento dei dati” e occupandosi di tutelare la persona solo contro pratiche di *profiling*[17] e contro quelle scelte adottate sulla base di processi di trattamento dati automatizzata[18]. Ma *quid iuris* nel caso in cui i dati personali fuoriusciti dalla sfera di dominio dell’individuo, continuino a essere utilizzati al di fuori del contesto nel quale erano forniti o si trasformino addirittura in tanti ulteriori *layer* di una rete neurale usata da un algoritmo di I.A..?

Siamo qui giunti al centro della questione. Il diritto alla cancellazione dei dati potrebbe essere interpretato estensivamente nel senso di spezzare il nesso tra passato e presente, anche in relazione all’informazione fatta propria da un algoritmo di *deep learning*? O fuoriesce, piuttosto, dallo scopo originario di tale diritto una siffatta tutela, dovendosi piuttosto affrontare il problema di una siffatta “appropriazione” dei dati esclusivamente dalla prospettiva del diritto della proprietà intellettuale? In altri termini, senza voler scendere nella questione dell’inquadramento giuridico di un algoritmo di *deep learning*, viene da chiedersi se la memoria che suddetta entità ha dell’informazione possa impattare sulla costruzione della identità del singolo nel contesto sociale, ovvero se il fatto che l’informazione sia priva di significato per la macchina escluda in *nuce* tale eventualità.

La risposta non è poi cosi scontata, laddove si osservi che se l’algoritmo è incosciente e al contempo intellegibile per la generalità delle persone, non lo è per gli *insiders* che lo hanno creato, i quali ben potrebbero, compiendo il percorso inverso, ricondurre l’informazione processata agli originali “dati personali”. Inoltre, la profilazione operata dell’algoritmo, attraverso un’autonoma reinterpretazione dei dati personali processati (AMOORE 2015), potrebbe alimentare il sentimento di essere categorizzati, schedati, etichettati, finendo per riflettersi sull’identità del singolo.

17 Cfr. Art. 4, comma 1, n. 4 del Regolamento (UE), ai sensi del quale deve intendersi per profilazione “qualsiasi forma di trattamento automatizzato di dati personali per valutare determinati aspetti personali relative a una persona fisica…”.
18 Cfr. Art. 22 del Regolamento (UE), ai sensi del quale “L’interessato ha diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significamente sulla sua persona”.

E il problema, a questo punto, riguarderebbe l'implementazione e l'*enforcement* di un tale diritto (CUSTERS 2016), posti gli elevati costi e tempi connessi all'individuazione dell'uso che dei dati personali viene fatto da macchine intelligenti.

5. Osservazioni conclusive. Fino ad oggi, nessuna innovazione tecnologica aveva messo in discussione così nel profondo il diritto della privacy come l'intelligenza artificiale. Tra i due, si è visto, s'istaurano complesse ingerenze reciproche. Infatti, da un lato, la I.A. nelle sue più moderne applicazioni moltiplica le possibilità di lesione della sfera individuale del singolo. Dall'altro, la privacy, nella sua moderna accezione di *data protection*, è divenuta non più e soltanto strumento a salvaguardia della propria sfera personale, ma strumento di regolazione economica.

Il legislatore europeo, in questo senso, ha adottato una disciplina che ha la presunzione di rafforzare il controllo del singolo sull'utilizzo dei propri dati e di estendere oltremodo il perimetro del suo ambito di applicazione.

Tale approccio, tuttavia, appare fortemente deficitario laddove si scontra con gli ultimi sviluppi in materia di I.A.. Da un lato, appare ingenua la pretesa di assicurare la trasparenza e il consenso informato a ogni tipo di trattamento, in un prevedibile scenario caratterizzato dall'uso sempre più estensivo di algoritmi non intellegibili dall'essere umano. Dall'altro, data l'assoluta centralità dei dati nello sviluppo di algoritmi di apprendimento automatico, deve sottolinearsi l'emersione di complesse sovrapposizioni tra *data protection* e proprietà intellettuale. Infatti, se i più moderni algoritmi di *machine learning* ottengono informazioni rilevanti a partire dai dati e al tempo stesso evolvono attraverso l'analisi di tali informazioni, sussiste un *trade-off* tra le opportunità connesse a un libero sfruttamento dei dati e i limiti derivanti dal riconoscimento di un elevato livello di *data protection*. Tale *trade-off* origina dalla diversa qualificazione della natura dei dati che, dalla prospettiva del moderno diritto della privacy, non devono considerarsi alla stregua di *commodity* scambiabili sul mercato. Questa diversità di vedute circa la natura dei dati è all'origine di una serie di problemi

quando si tratti di applicare la recente GDPR all'informazione processata da algoritmi di *machine learning*. Infatti, particolarmente critico risulta stabilire se il consenso al trattamento dei dati personali sia stato prestato per tutti gli usi che dei dati vengono fatti dagli algoritmi di *deep learning*. Ma, molto più critico, inoltre, è stabilire se il diritto alla cancellazione dei dati, previa revoca del consenso, possa trovare applicazione in questa materia o se l'"appropriazione" dei dati ad opera di un algoritmo di I.A. sia piuttosto questione del diritto della proprietà intellettuale. In relazione a questo problema, più che mai è necessario adottare una visione unitaria circa la natura dei dati, abbandonando l'approccio a compartimenti stagni che fino ad ora ha caratterizzato l'azione del legislatore e della dottrina. Infatti, in un'epoca dove i dati costituiscono la materia grezza della conoscenza, intaccando ogni settore economico e branca del diritto, lo sforzo del regolatore non può prescindere dall'elaborazione di una definizione comune di dati e da norme che cerchino di anticipare l'emersione di vuoti normativi e insanabili *clash* di discipline.

Riferimenti bibliografici

AMOORE L., PIOTUKH V., *Life beyond big data: Governing with little analytics*, in *Economy and Society*, vol. 44, 2015.

BALKIN J., *The Constitution in the National Surveillance State*, in *Minnesota Law Review*, vol. 93, 2008.

BALKIN J., *The Three Laws of Robotics in the Age of Bid Data*, in *Ohio St. L.J.*,vol 78., 2017.

BATESON G., *Steps to an Ecology of Mind*, Ballantine Books, New York, 1972.

CALO M. R., *Robots and Privacy*, in P. LIN, K. ABNEY, G. A. BEKEY (a cura di), *Robot Ethics: The Ethical and Social Implications of Robotics*, MIT Press, London, 2012.

CALO M. R., *People can be so fake: A new dimension to privacy and technology scholarship*, in *Penn. St. L. Rev.*, vol. 114, 2010.

CHEMERINSKY E., *Rediscovering Brandeis's Right to Privacy*, in *Brandeis L.J.*, vol. 45, 2007.

CUSTERS B., *Click here to consent forever: Expiry dates for informed consent*, in *Big Data & Society*, vol. 2, 2016.

DUMOUCHEL P., DAMIANO L., *Vivre avec les robots, Essai sur l'emphaties artificielle*, Seuil, 2016.

ESPOSITO E., *Algorithmic memory and the right to be forgotten on the web*, in *Big Data & Society*, 2017.

EKBIA H. R., *Artificial Dreams*, Cambridge University Press, New York, 2008.

GAVISON R., *Privacy & The Limits of Law*, in *Yale L.J.*, vol. 89, 1980.

KOOPS J. B., *Forgetting footprints, shunning shadows. A critical analysis of the right to be forgotten in big data practice. Scripted* 8 (3), 2011.

LATOUR B., *Social theory and the study of computerized work sites,* in W. J. ORLINOKOWSKI, G. WALSHAM (a cura di), *Information Techinology and Changes in Organizational Work*, Chapman and Hall, London, 1995.

MANES P., *Il consenso al trattamento dei dati personali,* Padova, 2001.
MAYER-SCHÖNBERGER V., CUKIER K., *Big Data. A Revolution That Will Transform How We Live, Work, and Think*, London: Murray, 2013.
MORMILE L., *Lo Statuto giuridico die dati personali*, in R. PANETTA (a cura di*), Libera Circolazione e protezione dei dati personali*, Giuffè, 2006.
OLIVO F., *Dati personali e situazioni giuridiche soggettive*, in *Giust. Civ*. vol. 4., 2002.
ORESTANO A., *La circolazione dei dati personali*, in R. PARDOLESI (a cura di), *Diritto alla Riservatezza e circolazione dei dati personali*, Giuffè, 2003.
PASQUALE F., *The Black Box Society, The Secret Algorithms That Control Money and Information*, Harvard University Press, London, 2015.
PIZZETTI F., *Il prisma del diritto all'oblio*, *Il caso del diritto all'oblio*, Torino, 2013.
RODOTÀ S., *Privacy e costruzione della sfera privata, Ipotesi e Prospettive*, in *Pol. Dir.*, 1991.
RUSSELL S., NORVIG P., *Artificial Intelligence: A modern Approach*, England: Pearson, Essex, 2009.
SAMUELSON P. A., *The Pure Theory of Public Expenditure*, in *The Review of Economics and Statistics*, 36, 387 ss, 1954.
SOLOVE D. J., *Speech, privacy and the reputation on the internet*, in M. NUSSBAUM, S. LEVMORE. *The offensive internet: Speech, Privacy and the Reputation*, Cambridge MA, MH Harvard U.P., 2011.
SINGER P. W., *Wired for War*, The Penguin Press, New York, 2009.
SPROULL L., *When the Interface is a Face*, in *Human – Computer Interaction*, vol. 11, 1996.
WARREN S. D., BRANDEIS L. D., *The right to privacy*, in *Harvard Law Review*, Vol. 4, No. 5, 1980.
WARWICK K., *Artificial Intelligence – The Basics*, Routledge, 2012.
WESTIN A., *Privacy and Freedom*, New York: Atheneum, 1970.
ZENO ZENCOVICH V., CODIGLIONE G. G., *Ten Legal perspectives on the "Big data revolution"*, in F. Di PORTO (a cura di), *Big data e concorrenza*, vol. 23, Giuffrè, 2016.
ZITTRAIN J., *The Future of the Internet: And How to Stop it*, Yale University Press, New Haven, 2008.

Il diritto alla portabilità dei dati. Tra diritti della persona a diritti del mercato

di **ANDREA GIULIA MONTELEONE**

SOMMARIO: **1.** INTRODUZIONE - **2.** IL DIRITTO ALLA PORTABILITÀ DEI DATI NEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI - **3.** LE LINEE-GUIDA DEL GRUPPO DI LAVORO ARTICOLO 29 - **4.** PORTABILITÀ DEI DATI COME RIMEDIO CONCORRENZIALE - **5.** CONCLUSIONI

Abstract

The General Data Protection Regulation (UE) 2016/679 extended the number of European citizens' rights with a new one: the data portability right. Article 20 of the Regulation, indeed, recognizes the right of data subjects to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. This right, born in response of a need to deal with the digital world practice to hamper users migration to other providers through technological lock-in, will be applicable to all the processing carried out by automated means based on data subject consent or on the execution of a contract and it is presumed to have a disruptive effect on online services market. Therefore, this work is aimed to examine the fundamental aspects of such a right with particular reference to the clarifications given by the Guidelines of Article 29 Data Protection Working Party and to the possible impact of the provision on competition.

1. Introduzione. Apparso originariamente come presidio libertario - e tecnologico - degli utenti dei social network e dei servizi di cloud storage, il diritto alla portabilità dei dati costituisce oggi un diritto dei cittadini europei in quanto riconosciuto espressamente dal Regolamento generale sulla protezione dei dati (RGPD) (SMARR - CANTER - SCOBLE - ARRINGTON 2007).[1]

Diventa, dunque, quanto mai interessante analizzare questo diritto di "nuova generazione" - un diritto 3.0 - alla luce del sistema della tutela dei dati personali, e dei risvolti concorrenziali che la disciplina di recente introduzione sembra avere.

1 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).

2. Il diritto alla portabilità dei dati nel Regolamento generale sulla protezione dei dati. Dopo un lungo periodo di gestazione, il Parlamento europeo ed il Consiglio, nell'aprile del 2016, hanno approvato il testo del Regolamento generale sulla protezione dei dati a sostituzione della precedente direttiva e con applicazione uniforme in tutti gli stati dell'Unione.[2]

Il testo è stato oggetto di una lunga discussione, sebbene le differenze rispetto alla precedente fonte normativa siano soprattutto tratte dall'elaborazione nazionale - ed europea - in materia. Tra le principali novità, e con natura assolutamente inedita, spicca senz'altro l'introduzione del diritto alla portabilità dei dati, cui è dedicato uno specifico articolo.

In particolare, l'art. 20 del RGPD prevede che:

"1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

2 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.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui".[3]

In altre parole, agli interessati dal trattamento è espressamente riconosciuto il diritto a che i titolari mettano a loro disposizione i dati di cui sono in possesso perché questi possano trasmetterli ad altri ed ulteriori titolari.

La portata del diritto, senz'altro dirompente, è tuttavia temperata dalla scelta del legislatore europeo di limitare i titolari a ciò obbligati alla duplice condizione che (i) il trattamento sia automatizzato; (ii) il trattamento sia giustificato dal consenso dell'interessato stesso o dall'esistenza di un contratto per la cui esecuzione sia necessario il trattamento di dati.

Questa previsione risponde ad un'esigenza diffusasi nella prassi - soprattutto nel contesto online - di poter agevolmente migrare da un servizio ad un altro senza che l'utente debba scegliere tra l'avvantaggiarsi dell'offerta di un diverso fornitore e la necessità di conservare i dati forniti e creati negli anni.[4] La decisione di introdurre un tale diritto è quindi coerente con la dichiara finalità di rafforzare i diritti degli interessati dal trattamento e, soprattutto, garantire un maggiore controllo degli stessi sui propri dati personali.[5]

La tutela intesa come controllo costituisce, d'altra parte, uno storico contraltare del tradizionale "right to be let alone" di Brandeis e Warren (TAVANI -

3 L'art. 84, § 5, del Regolamento (UE) 2016/679, facendo un espresso richiamo all'art. 20, fissa altresì il seguente quadro sanzionatorio: "(...) sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (...)".

4 La situazione tipica è la volontà dell'utente di passare ad un nuovo servizio telefonico, di somministrazione di luce, gas, acqua, servizi di posta elettronica, ma anche social network, cloud, ed in generale, qualsiasi servizio in cui l'aspetto reputazionale abbia una qualche rilevanza. D'altra parte, il diritto a che tale passaggio avvenga senza perdere quanto precedentemente acquisito, compiuto, costituisce la più piena realizzazione della libertà del consumatore in un mercato concorrenziale. Frequenti sono, invece, le c.d. data hostage clause, per degli esempi di tale clausola vedi: R.H. JR. CARPENTER, Walking From Cloud To Cloud: The Portability Issue In Cloud Computing, in Washington Journal of Law, Tech. & Arts, 6, 1, 2010

5 Considerando 68 del Regolamento (UE) 2016/679. Sul concetto di tutela come controllo, si segnalano altresì: GRUPPO DI LAVORO ARTICOLO 29, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 1 dicembre 2009, 02356/09/EN WP 168; COMMISSIONE EUROPEA, Comunicazione al Parlamento europeo, al Consiglio, Comitato Economico e Sociale e Comitati delle Regioni, A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final, Brussels, 4 novembre 2010; COMMISSIONE EUROPEA, Comunicazione al Parlamento Europeo, al Consiglio, Comitato Economico e Sociale e Comitati delle Regioni, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21th Century, COM (2012) 9 final, Brussels, 25 gennaio 2012.

MOOR 2000) (LAZARO - LE MÉTAYER 2015) (BRANDEIS - WARREN 1890, per la elaborazione tradizionale italiana, cfr. FERRARA SANTAMARIA 1937) ed in parte coincide con l'autodeterminazione informativa individuata dalla Corte Costituzionale tedesca quale diritto fondamentale della persona, secondo una teorizzazione poi fatta propria anche da altri ordinamenti e, da ultimo, indirettamente recepita anche nel RGPD.[6]

Il controllo, quindi, in questo nuovo contesto normativo, sembra sublimarsi concretizzandosi. Infatti, al controllo meramente giuridico, costituito dai tradizionali diritti di accesso,[7] correzione e cancellazione dei dati, il legislatore europeo affianca, anticipato dalla Corte di giustizia dell'Unione Europea, il diritto all'oblio e, sulla spinta delle summenzionate necessità tecnologiche, il diritto alla portabilità dei dati.[8] Quest'ultimo attribuisce materialità al controllo riconoscendo la possibilità all'interessato di vedere riuniti, in uno stesso formato, su uno stesso supporto, tutti i propri dati che siano nella disponibilità di un determinato titolare. Idealmente, dunque, questa facoltà da concretezza al principio di circolazione di dati come beni cui lo stesso titolo del RGPD rimanda.[9]

Tale concretizzazione, tuttavia, è ben lontana da un controllo proprietario in senso stretto, essendo il diritto alla portabilità soggetto a precisi e stringenti limiti.[10]

---

6 Volkszählungsurteil, Bundesverfassungsgericht 15 dicembre 1983, 1 BvR 209/83; Tribunale Costituzionale del Perù, sentenza n. 1846/2015.

7 B. CUSTERS - H. URSIC, Big data and data reuse: a taxonomy of data reuse for balancing data benefits and personal data protection, in International Data Privacy Law, 6, 1, 2016: "The right to data portability differs substantially from the pre-existing right to access. It extends beyond mere accessibility and emphasizes the importance of further data use and data reuse. In other words, data portability transforms passive data subjects into active reusers. A right to data portability empowers consumers to take advantage of value-added services from third parties and lets them 'share the wealth' created by big data".

8 Corte giust., C-131/12, Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González; B. CUSTERS - H. URSIC, Big data and data reuse: a taxonomy of data reuse for balancing data benefits and personal data protection, cit. : "Contrary to data sharing and data portability, which are described above as user controls, the right to be forgotten does not imply data reuse but rather deals with blocking all further, secondary uses".

9 Il Regolamento (UE) 2016/679 è definito "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".

10 Numerosi sono gli autori, soprattutto nel sistema di common law, che sostengono la necessità di ancorare la tutela dei dati personali all'istituto della proprietà, tra gli altri: J. LITMAN,

Alla delimitazione del diritto alla portabilità ha, infine, ulteriormente contribuito il Gruppo di Lavoro articolo 29. Infatti questo, dapprima nel dicembre 2016 e poi nuovamente il 5 aprile 2017, ha emanato delle linee-guida sull'argomento.

3. Le linee-giuida del Gruppo di lavoro articolo 29. Tra i primi documenti relativi al RGPD, il Gruppo di Lavoro articolo 29 ha ritenuto necessario produrre delle Linee-guida proprio relativamente al diritto alla portabilità e, sin dal principio del documento ha ritenuto massimamente opportuno chiarire che: "il diritto alla portabilità rappresenta anche uno strumento importante a supporto della libera circolazione dei dati personali nell'Ue e in favore della concorrenza fra i titolari. Questo nuovo diritto faciliterà il passaggio da un fornitore di servizi all'altro e potrà, quindi, favorire la creazione di nuovi servizi nel quadro della strategia per il mercato unico digitale".[11]

E ancora: "(i)l diritto in questione offre anche la possibilità di "riequilibrare" il rapporto fra interessati e titolari del trattamento tramite l'affermazione dei diritti e del controllo spettanti agli interessati in rapporto ai dati personali che li riguardano".[12]

Infine, è chiarito che il diritto alla portabilità costituisce un diritto nuovo da non confondere con la portabilità discussa e/o già attuata in altri ambiti normativi e con il più tradizionale diritto di accesso.[13]

Per quanto attiene più propriamente al merito, nella ricostruzione del Gruppo di Lavoro, il diritto alla portabilità si sostanzia nel: (i) ricevere i dati

---

Information Privacy/Information Property, in Stanford Law Review, 52, 2000: "Privacy can be cast as a property right. People should own information about themselves and, as owners of property, should be entitled to control what it is done with it"; V. BERGELSON, It's Personal but Is It Mine? Toward Property Rights in Personal Information, in 37 University of California Davis Law Review, 2003: "In order to protect privacy, individuals must secure control over their personal information by becoming real owners".

11 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", adottate il 13 dicembre 2016, versione emendata e adottata il 5 aprile 2017, 16/EN, WP 242 rev.01.

12 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", cit.

13 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", cit. Si fa espresso riferimento alla risoluzione contrattuale, al roaming nei servizi di comunicazione e all'accesso transfrontaliero ai servizi.

personali; e (ii) trasmettere dati personali da un titolare del trattamento ad un altro.

Ricevere i propri dati personali significa poterli conservare in vista del loro utilizzo pur in assenza di un immediato trasferimento ad ulteriore diverso titolare. Per questa ragione, i dati devono essere ricevuti, in ogni caso, "senza impedimenti", in formato "strutturato, di uso comune e leggibile da dispositivo automatico".[14] Quando poi la richiesta di portabilità è finalizzata ad un successivo trasferimento, questo deve avvenire "se tecnicamente fattibile" e, presumibilmente, tramite formati interoperabili.[15]

Sul titolare del trattamento grava oggi, quindi, l'onere di utilizzare formati strutturati ed interoperabili mentre non vi è alcun obbligo specifico di verificare la qualità dei dati prima di trasmetterli.[16] Spetta, invece, al titolare ricevente l'obbligo di verificare la correttezza, pertinenza e non eccedenza dei dati ricevuti.[17]

Ad ogni buon conto, il nodo centrale del dibattito in materia di diritto alla portabilità sta nella corretta individuazione dei dati rispetto ai quali il diritto può - e deve - essere fatto valere.

L'art. 20 RGPD, infatti, stabilisce che i dati portabili sono quelli che (i) riguardano l'interessato e (ii) quelli che siano stati forniti dall'interessato.

La prima condizione determina come diretta conseguenza l'inapplicabilità del diritto ai dati anonimi; la seconda, invece, determina non poca incertezza applicativa. Infatti, se da un punto di vista meramente teorico è pleonastico che siano forniti dall'interessato i dati forniti consapevolmente e attivamente, tuttavia, la prassi ci ha insegnato che l'interessato fornisce consapevolmente molti più dati di quelli che gli sono espressamente richiesti.

Pertanto, accanto alla categoria dei dati forniti attivamente, si pongono, nella ricostruzione del Gruppo di Lavoro, altre due specie di dati: quelli "osservati" dal titolare attraverso la fruizione del servizio da parte

14 Art. 20 del Regolamento (UE) 2016/679.
15 Art. 20 del Regolamento (UE) 2016/679 e Considerando 68 del Regolamento (UE) 2016/679.
16 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", cit.
17 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", cit.

dell'interessato e quelli "inferenziali e derivati creati dal titolare sulla base dei dati forniti dall'interessato".[18]

Il Gruppo di Lavoro, quindi, con l'esplicita finalità di non limitare eccessivamente la portata del diritto, conclude che "l'espressione 'forniti da' si riferisce ai dati personali relativi ad attività compiute dall'interessato o derivanti dall'osservazione del comportamento di tale interessato, con esclusione dei dati derivanti dalla successiva analisi di tale comportamento. Viceversa, tutti i dati personali che siano creati dal titolare nell'ambito di un trattamento, per esempio attraverso procedure di personalizzazione o finalizzate alla formulazione di raccomandazioni, o attraverso la categorizzazione o profilazione degli utenti, sono dati derivati o dedotti dai dati personali forniti dall'interessato e non ricadono nell'ambito del diritto alla portabilità".[19]

L'art. 20 RGPD, dispone altresì che dall'esercizio del diritto alla portabilità non deve derivare alcun pregiudizio agli altri diritti dell'interessato né determinare una lesione dei diritti di eventuali terzi.[20]

Questa necessità costituisce un altro aspetto certamente problematico, soprattutto rispetto alla necessità di tutelare con pari forza il medesimo diritto alla tutela dei dati personali di tutti gli eventuali terzi indirettamente coinvolti da una richiesta di portabilità. La risposta del Gruppo di Lavoro al proposito è particolarmente netta, escludendo radicalmente la possibilità per il titolare ultimo che riceve i dati di utilizzare i dati riferiti a terze parti per le proprie finalità. Per mitigare ciò, conclude il Gruppo, sarebbe opportuno consentire agli interessati di scegliere i dati su cui esercitare la portabilità anche in base alla necessità ed opportunità di trasferire dati di terze parti.[21]

---

18 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", cit.
19 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", cit.
20 Art. 20 del Regolamento (UE) 2016/679, § 4 fa espresso richiamo all'art. 17 del Regolamento (UE) 2016/679, diritto alla cancellazione o diritto all'oblio, recependo il suggerimento dell'European Data Protection Supervisor.
EUROPEAN DATA PROTECTION SUPERVISOR, Opinion on the data protection reform package, 7 marzo 2012: "The EDPS recommends that it is clarified in Article 18 that the exercise of the right to data portability is without prejudice to the obligation to delete data when they are no longer necessary, according to Article 5(e)".
21 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", cit.

4. Portabilità dei dati come rimedio concorrenziale. Oggetto delle Linee-guida del Gruppo di Lavoro articolo 29 è anche la modalità tramite cui i dati devono essere messi a disposizione sebbene chiarisca sin dal paragrafo introduttivo delle Linee-guida che "(s)eppure il diritto alla portabilità possa fungere da fattore di promozione della concorrenza fra i singoli servizi proprio perché facilita il passaggio da un servizio all'altro, il RGPD disciplina il trattamento dei dati personali e non la concorrenza fra le imprese".[22]

Proprio la necessità di individuare un formato se non comune, comunque interoperabile, ha fatto lungamente discutere la dottrina circa i risvolti concorrenziali che una tale imposizione potrebbe determinare, in quanto, così strutturato, il diritto alla portabilità potrebbe indirettamente (ed ingiustificatamente) imporre agli operatori di lavorare su medesimi formati.[23]
Per questo motivo, l'originaria formulazione del RGPD, che attribuiva alla Commissione il ruolo di individuare un formato comune di trasferimento, è stata abbandonata.[24]

Ciononostante, il Gruppo di Lavoro ritiene comunque necessario fornire dei chiarimenti al riguardo e, in particolare, enfatizzare il richiamo che il considerando 68[25] del RGPD fa all'interoperabilità che, in questa ottica,

22 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", cit.
23 È senz'altro più numeroso il fronte di chi, invece, sostiene che l'imposizione dell'interoperabilità sia favorevole alla concorrenza, tra gli altri, O. TENE - J. POLONETSKY, Big Data for All: Privacy and User Control in the Age of Analytics, in Northwestern Journal of Technology and Intellectual Property, 2013 "The importance of providing the data in a standard format according to industry-accepted guidelines. A standard, usable format fosters innovation by allowing software developers to create a single version of their product that will work for all utility customers across the country".
24 COMMISSIONE EUROPEA, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 gennaio 2012, COM (2012) 11 final, 2012/0011 (COD), articolo 18, § 3: "The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)".
25 Considerando 68 del Regolamento (UE) 2016/679: "Per rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. È opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati (…)".

costituisce l'obiettivo finale da raggiungere tramite un formato "strutturato", "di uso comune" e "leggibile da dispositivo automatico".[26] Tuttavia, si conclude affermando che "la portabilità intende produrre sistemi interoperabili, non sistemi compatibili" e che, in ogni caso "(i)l WP29 sostiene con forza la ricerca di forme di collaborazione fra i produttori e le associazioni di categoria al fine di sviluppare un insieme condiviso di standard e formati interoperabili che soddisfino i requisiti del diritto alla portabilità dei dati".[27]

Questo è proprio il cuore dell'intero diritto alla portabilità, realizzare una comunicazione tra sistemi per consentire agli utenti di evitare l'effetto lock-in, proprio di molti sistemi, che rende costoso – e talvolta impossibile – migrare da un sistema e/o un servizio ad un altro.[28]

Per questa ragione, il diritto alla portabilità è di interesse anche per il diritto della concorrenza.[29] D'altra parte, restrizioni al diritto alla portabilità, e quindi alla libertà dei singoli di passare senza costi di trasferimento da un servizio ad un altro, potrebbero essere strategicamente usate per acquistare e mantenere posizioni di dominanza e, per il tramite della negazione di interoperabilità, per realizzare condotte escludenti e sanzionabili ai sensi dell'art. 102 TFUE.[30]

---

26 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", cit.
27 GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", cit.
28 J. ALMUNIA, Competition and personal data protection, speech given at the Privacy Platform event: Competition and Privacy in Markets of Data, Brussels, 26 novembre 2012.: "The portability of data is important for those markets where effective competition requires that customers can switch by taking their own data with them".
29 B. ENGELS, Data portability among online platforms, in Internet Policy Review, 5, 2, 2016: "If data portability is not guaranteed, A can potentially preclude B from entering the market or from gaining a higher market share since users can only switch platforms at high costs if they cannot transfer their data"; nello stesso senso: COMMISSIONE EUROPEA, Working Paper, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25 gennaio 2012, SEC (2012) 72 final.
30 Al contempo, è ormai diffuso il convincimento che i dati costituiscano una vera propria infrastruttura, quindi sottoposta anche al regime delle essential facilities. In tal senso: OECD, Drawing value from data as an infrastructure, in Data-Driven Innovation: Big Data for Growth and Well-Being, OECD Publishing, Paris, 2015; G. COLANGELO, Big data, piattaforme digitali e antitrust, in Mercato Concorrenza Regole, 3, 2016; A. DIKER VANBERG - M.B. ÜNVER, The right to

Tale circostanza, quindi, potrebbe anche astrattamente determinare un vero e proprio conflitto di competenze tra autorità che sembravano avere poteri ed ambiti molto diversi: le autorità garanti della protezione dei dati personali e quelle garanti della concorrenza. D'altra parte, già il caso Facebook/Whatsapp ha svelato quanto i confini tra le diverse materie siano labili e quanto il diritto alla portabilità costituisca una questione di rilevanza concorrenziale.[31]

5. Conclusioni. Alla luce di tutto quanto sopra analizzato, sembra potersi concludere che come la tecnologia abbia reso necessaria l'esplicitazione del diritto alla portabilità, così sarà la tecnologia stessa ad incidere sulla sua effettività.

Infatti, la capacità degli operatori di individuare formati interoperabili e funzionali sarà determinante per l'effettivo riconoscimento del diritto alla portabilità dei dati.

Al contempo, non si può trascurare che l'autodeterminazione sia un processo quanto mai difficile e influenzato da una serie di fattori tra cui rivestono un ruolo cruciale sia la completezza dell'informazione che l'umana tendenza a deviare inconsciamente da comportamenti razionali.

Entrambe queste variabili, incidendo sulla consapevolezza dell'interessato rispetto al complesso dei propri dati trattati e all'esistenza stessa del diritto alla portabilità - come di qualsiasi altro diritto - potrebbero limitarne l'efficacia.

Ad ogni buon conto, sembra sempre più evidente che l'interessato dal trattamento non sia solo "interessato" ma vero e proprio titolare dei dati e, nella misura in cui può disporne, in un'accezione quasi proprietaria.

Il titolare del trattamento rimane al centro dell'attenzione del legislatore in quanto situato in una posizione di forza, e finanche in un mercato, ma è ormai evidente che non è affatto il centro della disciplina della tutela dei dati personali, essendo questo, invece, l'individuo nel suo duello contro la tecnologia.

---

data portability in the GDPR and EU competition law: odd couple or dynamic duo? , in European Journal of Law and Technology, 8, 1, 2017.

31 Case No COMP/M.7217, Facebook/WhatsApp, 3 ottobre 2014.

Riferimenti bibliografici

A. ACQUISTI - J. GROSSKLAGS, What Can Behavioral Economics, Teach Us About Privacy, in A. ACQUISTI, Digital Privacy. Theory, Technologies, and Practices, Auerbach Publications, New York, 2007.
J. ALMUNIA, Competition and personal data protection, speech given at the Privacy Platform event: Competition and Privacy in Markets of Data, Brussels, 26 novembre 2012.
AUTORITÉ DE LA CONCURRENCE - BUNDESKARTELLAMT, Competition law and data, 10 maggio 2016.
Y. BENHAMOU - L. TRAN, Circulation des biens numériques: de la commercialisation à la portabilité des données, in Sic !, 11, 2016.
V. BERGELSON, It's Personal but Is It Mine? Toward Property Rights in Personal Information, in 37 University of California Davis Law Review, 2003.
J. BICK, Big Data Rights Protection Found in Internet Copyright Law, in New Jersey Law Journal, 2015.
L. BRANDEIS - S. WARREN, The Right to Privacy, in Harvard Law Review, 4, 1890.
R.H. JR. CARPENTER, Walking From Cloud To Cloud: The Portability Issue In Cloud Computing, in Washington Journal of Law, Tech. & Arts, 6, 1, 2010.
A. CLEMENTE, Privacy, Cedam, Padova, 1999.
G. COLANGELO, Big data, piattaforme digitali e antitrust, in Mercato Concorrenza Regole, 3, 2016.
COMMISSIONE EUROPEA, Comunicazione al Parlamento europeo, al Consiglio, Comitato Economico e Sociale e Comitati delle Regioni, A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final, Brussels, 4 novembre 2010.
COMMISSIONE EUROPEA, Comunicazione al Parlamento Europeo, al Consiglio, Comitato Economico e Sociale e Comitati delle Regioni, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21th Century, COM (2012) 9 final, Brussels, 25 gennaio 2012.
COMMISSIONE EUROPEA, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 gennaio 2012, COM (2012) 11 final, 2012/0011 (COD).
COMMISSIONE EUROPEA, Working Paper, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25 gennaio 2012, SEC (2012) 72 final.
B. CUSTERS - H. URSIC, Big data and data reuse: a taxonomy of data reuse for balancing data benefits and personal data protection, in International Data Privacy Law, 6, 1, 2016.
A. DE FRANCESCHI - M. LEHMANN, Data as Tradeable Commodity and New Measures for their Protection, in The Italian Law Journal, 1, 2015.
A. DIKER VANBERG - M.B. ÜNVER, The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? , in European Journal of Law and Technology, 8, 1, 2017.
J. DREXL - R. M. HILTY - J. GLOBOCNIK - F. GREINER - D. KIM - H. RICHTER - P. R. SLOWINSKI - G. SURBLYTĖ - A. WALZ - K. WIEDEMANN, Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's ,"Public consultation on Building the European Data Economy", in Max Planck Institute for Innovation and Competition Research Paper, 9, 2, 2017.
B. ENGELS, Data portability among online platforms, in Internet Policy Review, 5, 2, 2016.
EUROPEAN DATA PROTECTION SUPERVISOR, Opinion on the data protection reform package, 7

marzo 2012.
M. FERRARA SANTAMARIA, Il diritto alla illesa intimità privata, in Riv. dir. civ., I, 168, 1937.
E. FIALOVA, Data Portability and Informational Self-Determination, in Masaryk University Journal f Law & Technology, 8, 1, 2014.
GRUPPO DI LAVORO ARTICOLO 29, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 1 dicembre 2009, 02356/09/EN WP 168.
GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sul diritto alla "portabilità dei dati", Adottate il 13 dicembre 2016, Versione emendata e adottata il 5 aprile 2017, 16/EN, WP 242 rev.01.
T. HOEREN, Big Data and the Ownership in Data: Recent Developments in Europe, in European Intellectual Property Review, 12, 2014.
F. KAREGAR - D. LINDEGREN - T. PULLS – S. FISCHER-HUBNER, Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track - Are People Ready for This?, in https://ifip-summerschool2016.hotell.kau.se.
W. KERBER, Digital markets, data, and privacy: Competition law, consumer law, and data protection, Joint Discussion Paper Series in Economics, 14, 2016.
C. LAZARO - D. LE MÉTAYER, The control over personal data: True remedy or fairy tale? , in SCRIPTed, 12, 1, 2015.
P. LEE - K. PICKERING, The general data protection regulation: a myth-buster, in Journal of Data Protection & Privacy, 1, 1, 5 agosto 2016.
J. LITMAN, Information Privacy/Information Property, in Stanford Law Review, 52, 2000.
V. MAYER - SCHOENBERGER - K. CUKIER, Big Data. Una rivoluzione che trasformerà il nostro modo di vivere – e già minaccia la nostra libertà, Garzanti, Milano, 2013.
OECD, OECD Internet Economy Outlook 2012, OECD Publishing, Paris, 2012.
OECD, Drawing value from data as an infrastructure, in Data-Driven Innovation: Big Data for Growth and Well-Being, OECD Publishing, Paris, 2015.
R.C. PICKER, Competition and Privacy in Web 2.0 and the Cloud, in Northwestern University Law Review Colloquy, 103, 2008.
S. RODOTÀ, Intervista su privacy e libertà, a cura di P. CONTI, Laterza, Roma - Bari, 2005.
I.S. RUBINSTEIN, Big Data: e End of Privacy or a New Beginning?, in New York University Public Law and Legal Theory Working Papers, 2012.
M. SKRINJAR VIDOVIC, EU data protection reform: challenges for cloud computing, in Croatian Yearbook of European Law & Policy, Vol.12, 2016.
J. SMARR - M. CANTER - R. SCOBLE - M. ARRINGTON, A Bill of Rights for Users of the Social Web, in www.template.org, 4 settembre 2007.
P. SWIRE - Y. LAGOS, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, in Maryland Law Review, 72, 2, 1, 2013.
H.T. TAVANI - J.H. MOOR, Privacy Protection, Control of Information, and Privacy -Enhancing Technologies, in ACM SIGCAS Computers & Society, 2000.
O. TENE - J. POLONETSKY, Big Data for All: Privacy and User Control in the Age of Analytics, in Northwestern Journal of Technology and Intellectual Property, 2013.
B. VAN DER AUWERMEULEN, How to attribute the right to data portability in Europe: A comparative analysis of legislations, in Computer law & security review, 2017.
S. WEISS, Privacy threat model for Data Portability in Social Network Applications, in International Journal of Information Management, 29, 4, 2009.
A. WIEBE, Protection of industrial data – a new property right for the digital economy?, in Journal of Intellectual Property Law & Practice, 12, 1, 2017.
C.S. YOO, When Antitrust Met Facebook, Penn Law, Faculty Scholarship, in George Mason Law Review, 19, 2012.
G. ZANFIR, The right to Data portability in the context of the EU data protection reform, In International Data Privacy Law, 1, 2012.
H. ZECH, Data as Tradeable Commodity, in A. DE FRANCESCHI, Europan Contract Law and the Digital Single Market, Intersentia, Cambridge, 2016.

Accountability principle under the GDPR: is data protection law moving from theory to practice?

by **ERNANI FRANCESCO CERASARO**

Abstract

Tra le molte novità introdotte dal nuovo Regolamento Generale sulla Protezione dei Dati, vi è è certamente l'affermazione normativa del principio dell'accountability, non esplicitamente previsto all'interno della previgente Direttiva 95/46/EC.
Il principio, non solo esige che il titolare del trattamento garantisca il rispetto delle disposizioni normative in materia di trattamento dei dati, ma richiede anche la concreta dimostrazione dell'adozione di adeguate misure legali, organizzative e tecniche a garanzia della tutela delle posizioni individuali.
Lo scopo di questo articolo è quello di dimostrare come l'introduzione di un siffatto principio costituisca un'opportunità per garantire l'effettività delle norme in materia di privacy, superando così l'incertezza giuridica che troppo spesso affligge il diritto fondamentale alla protezione dei dati personali.
Seguendo il *fil rouge* dell'effettività, sarà poi possibile analizzare gli effetti più rilevanti derivanti dall'applicazione del principio dell'accountability: l'adozione di un approccio basato sul rischio ed il conseguente obbligo di fornire una valutazione dell'impatto sulla protezione dei dati.

1. Accountability principle as a natural follow-up of the need for trust. Rapid technological developments and globalisation have brought new challenges for the protection of personal data. Those developments required a stronger and more coherent data protection framework in the European Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market[1]. Since the protection of personal data was regulated by the Directive 95/46/EC, which dates back to 20 years ago and therefore was too obsolete and inadequate to regulate such a dynamic and technological-dependent topic (MAGUIRE S., 2015), a reform in the regulatory framework was almost mandatory.

In fact, even if the core objectives and principles of the former Directive remain valid, it has not prevented, among others, three substantial problems:

1 Cfr. Recital n.7 of the GDPR

fragmentation in the implementation of data protection across the Union; legal uncertainty; a general public perception that there were significant risks to the protection of natural persons[2].

So, after four long years of negotiations, the European legislator adopted the GDPR[3], replacing the former Directive.

The new Regulation, is designed to harmonize data privacy laws across Europe and to ensure a satisfactory protection also outside the Union[4]; to protect and empower all EU citizens; and to reshape the way in which organizations, citizens, companies and freelancers approach to data protection and privacy.

What these general issues have in common is the necessity of an effective protection of individual positions, mainly because with the relentless technological development we face every day, processing of personal data is increasingly becoming dependent on the ubiquity of the data flow.

This needed new rules and procedures[5], which hopefully are more appropriate to regulate this absence of an individuated or detectable geographical regulatory area.

After a careful reading of the new legislation, what become evident is that the European legislator, attempting to translate in practice the many-parties requests formulated in the previous years, has adopted a legal framework which follows the primary and general objective of the trust-building in relations between data subject, controllers, processors and in general all the actors involved.

---

2 Cfr. Recital n.9 of the GDPR: The present differences in the level of protection of the right to the protection of personal data may prevent the free flow of personal data throughout the Union and therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law.

3 European Regulation (EU) 2016/679

4 A first and essential element of the new legislation is that it is a Regulation, which results in its direct applicability in all Member States, without the adoption of a legislative provision at national level. Furthermore, the Regulation will apply to companies which, although located outside the Union territory, offer services or products to persons within one of the Member States.

5 On this regard, a fundamental step is that the Europeanization of the legislation will not only affect rules, but also processes (e.g.: the introduction of the Stop-shop principle, according to which companies operating in different territories can address their requests and their claims to a single national DPA, will ensure huge savings and uniformity in the application of the laws).

In trying to provide an effective and efficient protection of personal data in a socio-economic context that is constantly changing, data protection enters in a new era, in which all the data controllers and processors will be subject to new obligations, including the adoption of internal policies, mechanisms to implement privacy policies, internal oversight systems, transparency and remediation.

The GDPR introduces new rights for citizens, which will be fully respected only if it will be ensured the effective application of the new obligations provided for data controllers.

This means, in a very a-technical way, that individuals' rights depend on the willingness of data controllers in doing their homework, far more than before.

In other words, GDPR's «cornerstone is the concept of trust: trust in data controllers to treat personal information responsibly, and trust that the rules will be effectively enforced» (BUTTARELLI G., 2016).

The material consequence of the regulatory importance of the concept of trust is the formal introduction of the principle of "accountability" within the GDPR.

This is an important recognition at the regulatory level of a principle which was recognized solely from a theoretical point of view, as a way to regulate and self-regulate privacy responsibilities exercised by organizations.
The theoretical concept of privacy accountability, as a model, «is a set of activities (dimensions) that should be undertaken by (...) organizations in order to become a privacy-accountable entity» (RABAN Y., 2012)[6].

6 *«This model includes dimensions and indicators (concrete activities) as follows:a) Planning, awareness building, conceiving and strategizing related to privacy (reflexivity). Such activities may be fulfilled by appointing a privacy officer, by conducting regular consulting cycles regarding privacy and by the execution of privacy impact assessments.b) Making privacy-related information available to the public (information availability). Indicators for information availability may include privacy statements, codes of ethics, the use of Transparency Enhancing Technologies (TETs), and compliance reports.*
c) Exercising two-sided communication with stakeholders, including citizens, on issues of privacy (communicability). Indicators of communicability may include hotlines, discussions in forums and social media such as Facebook where issues discussed may include ethics and privacy.

More generally, with respect to a norm, «a relationship qualifies as a case of accountability with respect to an obligation when: there is a relationship between an actor and a forum, in which the actor is obliged to report, explain, and justify his conduct relative to the norm, the forum can pose questions, pass judgement, and the actor may face consequences» (RAAB C., 2017).

In order to fully understand the reason of the introduction of such a principle to regulate data protection, it should take a few steps back in the years.

The accountability privacy principle appeared the first time in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, in which was already present the taste of a lack of effectiveness in the protection of individual privacy.

Guidelines stated that a «data controller should be accountable for complying with measures which give effect to the principles» of the data protection. This means that the organization that collects the personal data responsible for the data while it or its agents have control or custody of the data.

From a "statutory" perspective, the first appearance of the principle was in the Personal Information Protection and Electronic Documents Act in the Canadian Fair Information Principles. The principle required to develop and implement policies and practices to uphold the 10 Fair Information Principles, including implementing procedures for protecting personal information and establishing procedures for receiving and responding to complaints and inquiries.

Then, in 2010, the Article 29 Working Party (WP29) complained more expressly about the necessity to add in the regulatory framework some additional tools to ensure the effectiveness in the application of privacy laws.

---

d) Changing the behavior of security organizations with respect to privacy (action-ability). This may be indicated by the enabling of citizen's requirements to be implemented through focus groups or citizen's juries. Other indicators may simply be changes in products due to Privacy by Design (PbD), or the introduction of privacy enhancing technologies.
e) Evidencing and verification of privacy accountability (testability). Indicators may include compliance with standards and regulations, including compliance with self-regulation mechanisms».

In particular, in the opinion 3/2010, the WP29 pitched a concrete proposal for a regulatory recognition of the accountability principle «which would require data controllers to put in place appropriate and effective measures to ensure that the principles and obligations set out in the Directive (95/46/CE) are complied with and to demonstrate so to supervisory authorities upon request. This should contribute to moving data protection from 'theory to practice' as well as helping data protection authorities in their supervision and enforcement tasks»[7].

In that opinion, WP29 explained, on one hand, how the accountability principle can bring to legal certainty; on the other, it highlighted how such principle could impact other areas, including international data transfers, notification requirements, sanctions, and eventually also the development of certification programs or seals.

In its conclusions, the WP29 stressed that «the increase of both the risks and the value of personal data per se support the need to strengthen the role and responsibility of data controllers». It was clear then that a possible future regulation had to contain the necessary tools to encourage data controllers to apply in practice appropriate and effective measures that deliver the outcomes of the data protection principles.

Six years after that, by adopting the GDPR, the European legislator has almost exhaustively implemented the advice pushed forward by WP29.

With the GDPR, accountability, as a data protection principle, «gained fresh prominence» (JASMONTAITE L., VERDOODT V., 2016) and became a keystone of the data regulatory framework.

Accountability is now expressly recognized in the art. 5, second paragraph, of the Regulation, where the data controller is identified as the competent person to ensure compliance with the principles laid down in the first subparagraph of the same article (lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality).

7 WP29 Opinion 3/2010.

The data controller, moreover - and perhaps in this is entailed the most important novelty, as well as it is the core of the principle of accountability - will have not only to ensure compliance with the principles, but he will also have to "demonstrate" such compliance.

The controller will be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with the Regulation, including the effectiveness of the measures[8].

The accountability of data controller is further specified in the article 24 of the Regulation, bearing the "Responsibility of the controller", which provides that «taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" Those measures shall be reviewed and updated where necessary»[9].

In other words, «an organization must be responsible for personal information and be able to "account for it" within the organization and when it flows to business partners (vendors and service providers) by being able to demonstrate the status of their privacy program to internal stakeholders such as senior management and, if desired (or required), to external stakeholders such as regulators, commissioners, data protection authorities, attorneys general and business partners»[10].

So, the principle of accountability, on the one hand, restores the discretion of the controller to the identification of the measures considered to be more appropriate, while taking into account the above-mentioned criteria; on the other hand, the controller is the same person who deals with the concrete demonstration of the necessity and adequacy of the measures chosen.

8 Recital 74 of the GDPR

9 In the Italian regulatory landscape, requiring the data controller to take appropriate measures, taking into account the characteristics of processing, goes beyond the prevailing discipline contained in Annex B to the italian Privacy Code where more general "minimum measures" were required.

10 https://iapp.org/news/a/demonstrating-privacy-accountability/

The principle of accountability, however, is not limited only to compliance and to its concrete demonstration through appropriate and adequate measures.

Accountability is far more complex and catchy than this.

It sets a higher standard than compliance, and be subject to rules is not enough.

The recognition of accountability as a principle raises socio-cultural reflections, which could lead to a paradigmatic change in how to conceive the protection of personal data.

Data protection seems moving from a static and rigid view to a dynamic and flexible one in which all involved actors are accountable.

Accountability is a paradigmatic change in how to approach data protection. Accountability is the foundation for a social policy change in the affirmation of the fundamental right to the protection of personal data. Therefore, accountability «is an opportunity: if properly implemented, it is an incredible tool to implement tailor-made and personalized measures adopted to the specificities of each organisations, in order to make data protection more effective» (BUTTARELLI G., 2017).

2. Concretizing accountability: risk based approach and DPIA. The principle of accountability can be taken as a theoretical basis of a number of some (more or less) concrete obligations that should ensure effective compliance with the regulatory provisions, resulting otherwise in risks for data subject, with different probabilities and severity. Such risks are likely to cause physical, material or immaterial damage (discrimination, identity theft, financial loss, reputation damage, loss of confidentiality of personal data protected by professional secrecy, etc.)

The risk of treatment is therefore not a novelty in the privacy law scene.

However, what is certainly an important novelty, is the centrality that the figure of the risk assumes within the new Regulation due to the adoption of the “accountable” approach.

While, on the one hand, it is true that the concept of "risk" was already present within the Directive 95/46/EC, on the other hand, it is equally true that with the GDPR the risk assessment becomes an indispensable tool to correctly process personal data.

In doing so, the Regulation would seem to overcome the Directive95/46/EC which providing for a general obligation to notify the control authorities of the processing has not always helped to improve the protection of personal data.

The European legislator considered then appropriate to abolish these general and indiscriminate notification obligations and replace them with procedures focused on identifying treatments that potentially pose a high risk to the rights and freedoms of natural persons by their nature, scope, application, context and purpose, by introducing the "risk-based approach".

By adopting this approach, the GDPR encourages organizations and companies to evaluate in advance the strength and probability of the risk, in order to facilitate the adoption of appropriate and effective measures.
Appropriate and effective because they essentially correspond to the level of risk.

This does not mean that the protection of individual rights will depend solely on the level of risk involved with the activity which it is referred to, but that in order to effectively protect individual positions, it is necessary for the data subjects to modulate the adoption of the necessary measures relying on risk assessments.

From a different point of view, a preventive risk assessment can only benefit organizations handling data, as it will be possible for them to concentrate their efforts on the most risky activities, maximizing the possible benefits of a treatment-related activities.

In other words, such approach could ultimately help to overcome the abstractness and nebulosity of some privacy regulations.

In fact, the Regulation introduces the Data Protection Impact Assessment (DPIA), a fundamental procedure «in order to define an adequate strategy to limit privacy risks» (MANTELERO A., 2013).

It is an instrument designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.

DPIAs ensure that «a conscious and systematic effort is made to assess privacy risks to individuals in the collection, use and disclosure of their personal data. DPIAs help identify privacy risks, foresee problems and bring forward solutions»[11].

As the WP29 has underlined in its guidelines, «DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance»[12].

In accordance with Article 35, the DPIA must be carried out in presence of those situations in which the processing of data, because of its nature, scope, context and purpose A DPIA is only required when the processing is *«likely to result in a high risk to the rights and freedoms of natural persons»*.

There is no definition of "high risk" under the GDPR, but Article 35(3) provides some non- exhaustive examples of processing activities in which processing is "*likely to result in a high risk"*:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

11 Commission Staff Working Paper - Impact Assessment /* SEC/2012/0072 final.
12 WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, published on 4 April 2017.

b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

c) a systematic monitoring of a publicly accessible area on a large scale.

In such cases, the data controller should carry out a prognostic evaluation of the impact that the treatment might have on the affected persons.

More specifically, the DPIA must contain, as minimum features[13]: a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller; an assessment of the necessity and proportionality of the processing in relation to the purpose; an assessment of the risks to individuals.

This impact assessment should also cover measures, guarantees and mechanisms designed to mitigate this risk, including security and to demonstrate compliance, thus ensuring the protection of personal data and demonstrating compliance with the Regulation.

As a result of this evaluation, a number of alternatives are more or less analytically described in the Regulation.

First, where the assessment would result that treatment could pose a high risk to the rights and freedoms of natural persons and the data subject was of the opinion that the risk could not be reasonably mitigated in terms of available technologies and implementation costs. The Regulation considers appropriate that the holder contacts the supervisory authority prior to the start of the treatment activities.

The supervisory authority that receives the request for consultation should do so within a specified time limit.

A DPIA may concern mostly a single data processing operation. However, Article 35(1) states that «a single assessment may address a set of similar processing operations that present similar high risks». Recital 92 adds that there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a

13 Article 35(7), and recitals 84 and 90

single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

DPIA is certainly an important instrument to ensure effectiveness to the application of the principle of accountability.

In fact, under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)), carrying out a DPIA in an wrong way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can each result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher[14].

Conclusively, the impact assessment, using a «three-phase model focused on prescription, ex post evaluation, and sanction», «is able to generate privacy oriented solutions, offering a high level of data protection and, in this way, it contributes to increasing users' trust in technology and its related services» (MANTELERO A., 2013).

3. Conclusions. As the European Data Protection Supervisor Giovanni Buttarelli highlights, the GDPR's «cornerstone is the concept of trust» (BUTTARELLI G, 2016).

Relying on this concept, the Regulation introduces in the regulatory framework the principle of accountability, which constitutes a tangible normative intent to move data protection from theory to practice.

In fact, even if «Accountability has been perceived as a soft approach to data protection (...) (it) requires hard work, continuous review and a complete understanding of your data flows» (BERMÚDEZ J.A., 2015).

14 Cfr. Cit. WP29 Opinion, p. 8.

The centrality of accountability in data management is then undoubtedly one of the most challenges in applying the new Regulation.

At the same time, «accountability may be neither a necessary nor a sufficient condition for trust. In order to provide an improved basis for trustworthiness via enhancing accountability, certain conditions need to be met» (PEARSON S., 2017).

Accountability does not redefine completely privacy or replace laws.

It «shifts the focus of privacy governance to an organization's ability to demonstrate its capacity to achieve specified privacy objectives»[15].

In other words, «figuratively, accountability is the flu vaccine for the data protection immune system. When an organisation has the data protection sniffles, accountability, like the flu vaccine, enhances the immune system» (ABRAMS M., 2017).

Nevertheless, accountability can be taken as a driver for effective implementation of data protection principles, not as a magic stick.

It is then imperative to carry out a cultural shift in the approach to data management.

This «means a change to the culture of an organisation. That isn't an easy thing to do, and it's certainly true that accountability cannot be bolted on: it needs to be a part of the company's overall systems approach to how it manages and processes personal data. But this shift in approach is what is needed. It is what consumers expect. The benefit for organisations is not just compliance but also providing an opportunity to develop the trust of its consumers in a sustained way» (DENHAM E., 2017).

The new Regulation, following a trust-building approach, represents an opportunity for growth for all the actors: data subject, regulators, businesses, etc.

But as in life, so in law, growing involves responsibility.

Therefore, the GDPR rightly requires more proactivity, which concretizes in accountability and in a risk-based approach.

15 https://iapp.org/resources/article/accountability-5/

The effective reception of these normative and conceptual innovations will be an important crossroads for the future of European citizens, increasingly subjected to threatening data processes they ignore, requiring therefore the most real and concrete guarantees.

However, without a strong inversion of cultural tendencies within all the actors involved, nothing will significantly change.

The year which separates us from the full applicability of the Regulation will be fundamental. It will show us if the necessity of such a cultural shift is already internalized.

Riferimenti bibliografici

G. BUTTARELLI, *The EU GDPR as a clarion call for a new global digital gold standard,* International Data Privacy Law 6.2 (2016): pp. 77-78.
G.BUTTARELLI, *Hitting the ground running: How regulators and businesses can really put data protection accountability into practice*, Keynote speech at European Data Protection Days (EDPD) Conference Berlin, 15 May 2017
E. DENHAM, delivered this speech at a lecture for the Institute of Chartered Accountants in England and Wales in London on 17 January 2017. She discussed the role of accountability in the GDPR, underlining that "*We're all going to have to change how we think about data protection".*
L. JASMONTAITE, V. VERDOODT, *Accountability in the EU Data Protection Reform: Balancing Citizens' and Business' Rights. Privacy and Identity Management. Time for a Revolution?*,
S. MAGUIRE, *A metadata-based architecture for user-centered data accountability*, Electronic Markets 25.2 (2015): 155-160: «Data is rapidly changing how companies operate, offering them new business opportunities as they generate increasingly sophisticated insights from the analysis of an ever-increasing pool of information. Businesses have clearly moved beyond a focus on data collection to data use, but users have an inadequate model of notice and consent at the point of data collection to limit inappropriate use»
A. MANTELERO, *Competitive value of data protection: the impact of data protection regulation on online behavior,* International Data Privacy Law (2013), 3(4): 229-238. http://dx.doi.org/10.1093/idpl/ipt016, pp.234-326.
S. PEARSON, *Strong Accountability and Its Contribution to Trustworthy Data Handling in the Information Society. IFIP International Conference on Trust Management*. Springer, Cham, 2017.
Y. RABAN, *Privacy Accountability Model and Policy for Security Organizations (2012*[1] C. Raab, *Information Privacy: Ethics and Accountability, Ethik in den Kulturen-Kulturen in der Ethik: Eine Festschrift für Regina Ammicht Quinn* (2017), p. 335.

Sitografia

https://iapp.org/resources/article/accountability-5/
http://informationaccountability.org/time-to-double-down-on-accountability/

LUISS Law Review - Rivista online del centro di ricerca LUISS DREAM
Dipartimento di Giurisprudenza LUISS Guido Carli
Registrata presso il Tribunale di Roma con il n. 65/2016
ISSN 2531-6915
Direttore responsabile: Gian Domenico Mosco
Responsabile di redazione: Raffaella Scarabino
LUISS Guido Carli - Viale Pola, 12, 00198 Roma, Italia P.I. 01067231009

LUISS DREAM
Diritto e Regole per Europa
Amministrazione e Mercati