Diritto, Economia e Tecnologie della Privacy

Anno VI, Numero 2, 2015

Istituto Italiano Privacy

Diritto, Economia e Tecnologie della Privacy

Rivista quadrimestrale dell'Istituto Italiano per la Privacy e la valorizzazione dei dati

Diritto, Economia e Tecnologie della Privacy

Anno VI, n. 2, 2015
Registrazione al Tribunale di Arezzo n. 1P/10RS del 26 ottobre 2010
Rivista quadrimestrale

Provider: Aruba S.p.A., P.zza Garibaldi 8 – 52010 Soci (AR). Autorizzazione Ministero delle Comunicazioni n. 473. Server collocati in Via Sergio Ramelli, 8 – 52100 Arezzo (AR).
Stampa: Daniele Mosera, via Giulio Pittarelli, 23, 00166, Roma.

Segreteria di redazione:
e-mail: rivista@istitutoitalianoprivacy.it

Direzione e redazione: Piazza di San Salvatore in Lauro, 13, 00186, Roma; Direttore responsabile: Giovanni Crea

Proprietà della rivista: Istituto Italiano per la Privacy e la valorizzazione dei dati. Consiglio di Amministrazione dell'Istituto Italiano per la Privacy e la valorizzazione dei dati: Luca Bolognini – Presidente; Diego Fulco – Direttore; Pietro Paganini – Segretario Generale.

Editore: Istituto Italiano per la Privacy e la valorizzazione dei dati, Piazza di San Salvatore in Lauro, 13, 00186, Roma
www.istitutoitalianoprivacy.it
info@istitutoitalianoprivacy.org
tel.: +39 06 97842491
fax: +39 06 23328983

Condizioni economiche

- singolo numero: € 25,00
- abbonamento annuale (tre numeri): € 70,00 (L'abbonamento decorre dal mese di gennaio di ciascun anno. La sottoscrizione dell'abbonamento nel corso dell'anno dà diritto a ricevere i numeri arretrati). Il pagamento può essere effettuato mediante versamento bancario sul conto intestato a Istituto Italiano per la Privacy e la valorizzazione dei dati – IBAN – IT55V0310450120000000821176 (Deutsche Bank)

INDICE

Editoriale

Networking e ubiquitous data computing. Strutturazione e caratteristiche degli ambienti intelligenti

GIOVANNI CREA

Il processo di espansione delle tecnologie dell'informazione e della comunicazione è iniziato dal versante sociale, con l'obiettivo di spostare nella dimensione digitale buona parte delle funzioni che famiglie, imprese e pubbliche amministrazioni hanno sempre svolto con modalità tradizionali; una tale finalità – che in Europa rimonta alla "Strategia di Lisbona" – viene rappresentata con un modello socioeconomico con cui studiosi e *policy maker* descrivono l'integrazione delle ICT nei settori pubblico e privato, esaltandone le capacità di trattamento (*computing*) delle informazioni e delle conoscenze e di trasporto delle stesse[1]. Questo processo si sta svolgendo con tutti i suoi profili di complessità legati, in particolare, all'avvento del *web 2.0* che ha innescato un'incontrollabile circolazione di contenuti ed ai motori di ricerca che ne facilitano il reperimento; sappiamo, al riguardo, come tale complessità abbia offerto il fianco alle ben note questioni di carattere regolamentare legate all'individuazione, tutt'altro che scontata, delle figure a cui

[1] In letteratura si veda A. MATTELART, *Storia della società dell'informazione*, Torino, 2002; D. LYON, *La società dell'informazione*, Bologna, 1991; D. FORAY, *L'économie de la connaissance*, Paris, La Découverte Repères, 2000; F. MACHLUP, *Knowledge, its creation, distribution and economic significance*, Princeton, Princeton University Press, 1984. Sul mutamento della società verso un modello *network* si veda M. CASTELLS, *La nascita della società in rete*, Milano, 2002. Nel quadro delle politiche comunitarie in tema di diffusione delle ICT si rinvia a COMMISSION OF THE EUROPEAN COMMUNITIES, *Growth, competitiveness, employment. The challenges and ways forward into the 21st century*, Brussels, 1993 (comunicazione COM(93) 700, del 5 dicembre 1993, libro bianco di Jacques Delors); Raccomandazione al Consiglio europeo, *Europe and the global information society*, Bruxelles, 26 maggio 1994 (c.d. rapporto Bangemann). Il libro bianco di Delors e il rapporto Bangemann hanno posto le premesse l'adozione della strategia di Lisbona.

attribuire le responsabilità dei comportamenti in rete[2]; questioni che introducono condizioni di incertezza per i consumatori concernenti i livelli di servizio, la protezione dei dati personali, la tutela dei minori che utilizzano internet, prospettando pertanto un vera e propria crisi della regolamentazione. Peraltro, va anche osservato che il modello socioeconomico appena descritto si caratterizza per la sua predisposizione alla *law and technologies* o – per dirla con le parole di Lawrence Lessig – al regime del *code*[3], in ragione dello strato delle ICT da cui dipende in larga parte il suo funzionamento. Sotto questo profilo, il diritto deve garantire l'adozione di misure *software*, possibilmente progettate in modo da agire *ex ante*, ponendo vincoli e impedendo comportamenti contrari alle norme. Da qualche tempo, poi, le traiettorie evolutive delle ICT puntano a una compenetrazione anche tra gli elementi "non cognitivi" dell'ambiente che, in tale prospettiva, acquisirebbero un'intelligenza artificiale, rappresentata dalla capacità di codificare in forma digitale, con l'ausilio del *software*, la realtà circostante (luoghi, accadimenti, comportamenti) – e dunque, di tradurla in informazioni – e di scambiare, attraverso la rete, i contenuti informativi che riassumono tale realtà. Le tecnologie *Radio frequency identification* (RFID) ovvero le *Global positioning system* (GPS) o, ancora, le *Wireless fidelity* (WI-FI) sono esempi emblematici di ICT la cui integrazione nell'ambiente, in chiave *everythings*, implica la produzione di notevoli quantità di contenuti informativi, e di cui, da qualche tempo, si discutono le opportunità di sfruttamento per la ricerca, la crescita economica sostenibile, la prevenzione di fenomeni naturali avversi, la qualità della vita[4]. A tal

[2] In tal senso, con riguardo al settore energetico, si veda GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 12/2011 sui contatori intelligenti (smart metering)*, 4 aprile 2011.

[3] Cfr. L. LESSIG, *Code and other law of cyberspace*, New York, 1999. Sull'argomento si veda anche il saggio di G. ZICCARDI, *Il controllo del codice informatico tra diritti, etica e business*, in *Rivista Politeia*, n. 82/2006, nonché N. LETTIERI, *Ambient intelligence: breve introduzione alla tecnologia silenziosa ed alle sue proiezioni sul piano giuridico*, in *Informatica e diritto*, n. 1-2, 2008, 119-132.

[4] In tal senso il *Parere del Comitato economico e sociale europeo in merito alla «Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – Verso una florida economia basata sui dati»*, in *GUUE*, C 242, 23 luglio 2015, p. 61. In

riguardo, va sottolineato come una parte della letteratura, utilizzando un'accezione allargata, tenda a descrivere i sistemi di ICT alla stregua di "infrastrutture cognitive"[5] le cui funzioni denotano un'intelligenza (invero) programmata che si integra con le capacità umane (immaginazione, creatività, correlazione), in tal modo dando forma a processi cognitivi combinati. L'evoluzione che va delineandosi descrive pertanto la prospettiva di ambienti «intelligenti» – spesso indicati con il termine *smart* – aventi una struttura reticolare i cui 'nodi' sono rappresentati da sistemi (viventi e non) che producono, scambiano e riutilizzano risorse informative e conoscitive. Il modello *smart* – già preconizzato da Mark Weiser nel 1988 attraverso il paradigma dell'elaborazione pervasiva (*ubiquitous computing*), integrata con l'ambiente[6] – va dunque oltre la concezione di un impiego delle tecnologie che sia esclusivo dell'uomo prospettando il definirsi di sistemi «cognitivi» allargati a macchine, strumenti, beni di consumo durevoli (elettrodomestici), impianti, capaci di produrre e di processare anche autonomamente informazioni e conoscenze. Sotto quest'ultimo aspetto, va osservato come, in talune circostanze, la sostituzione dell'operatività umana con l'intelligenza di determinati elementi dell'ambiente appaia opportuna, ad esempio sotto il profilo economico con l'eliminazione di costi legati a una costante presenza dell'uomo[7]. Le caratteristiche di *networking* e di pervasività dei sistemi cognitivi testé tratteggiati lasciano intuire una tendenza che si collega al fenomeno della globalizzazione e che, per questo, va

letteratura, si veda C. CAPINERI, A. RONDINONE, *Geografie (in)volontarie*, in *Rivista geografica italiana*, n. 3, 2011, 559-577.

[5] In tal senso, con riguardo ai processi di apprendimento, G. OLIMPO, *Società della conoscenza, educazione, tecnologia*, in *Tecnologie didattiche*, vol. 18, n. 2, 2010, 4-16. Cfr. anche J. MITOLA, G.Q-MAGUIRE, *Cognitive radio: making software radios more personal*, in *IEEE personal communications*, vol. 6, n. 4, 1999; I. ENRICI, *La dimensione psicologica nella sicurezza: un approccio cognitivo*, Santarcangelo di Romagna, Maggioli, 2011.

[6] Cfr. M. WEISER, *The computer for the 21st century*, in *Scientific American*, n. 3, 1991, 94-104. Sul paradigma *ubiquitous computing* si veda anche S. LEVIALDI, *I nuovi percorsi dell'interazione uomo-macchina*, in *Mondo digitale*, n. 1, 2006, 36-46.

[7] Sul punto si veda AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI, *Future Internet: scenari di convergenza, fattori abilitanti e nuovi servizi*, 3 marzo 2014.

considerata alla stregua di una strategia di adattamento (e sopravvivenza) ai processi di unificazione economica, culturale, geopolitica. In questo quadro, il trattamento delle informazioni e delle conoscenze riveste una funzione essenziale, descrivendo un processo produttivo che si svolge nei nodi della rete e il cui *output* è rappresentato da nuova conoscenza. E ciò spiega lo spostamento su questa risorsa degli investimenti dell'epoca *post*-industriale, in tal modo modificando l'originaria impronta industriale del capitalismo che la letteratura sull'economia della conoscenza ha classificato come "capitalismo cognitivo" ovvero "capitalismo delle reti"[8].

Il paradigma delle realtà intelligenti riposa dunque su esigenze di *networking* e di *data computing* che originano dalla consapevolezza che la rete rappresenta un'entità cognitiva superiore che, più delle sue parti costituenti, è capace di affrontare la complessità della globalizzazione. Al contempo, lo stesso paradigma ripropone su un piano decisamente più impegnativo la questione del bilanciamento con quegli interessi che richiedono di limitare il trattamento e la circolazione dei contenuti informativi e conoscitivi. Sotto questo profilo, va rilevato come le reti cognitive estese – che implicano un'ampia partecipazione sia di imprese dell'industria delle ICT (*internet service provider*, operatori di telecomunicazioni, produttori di *software*) sia dei settori che si avvalgono delle ICT (*public utilities*, infrastrutture critiche, assicurazioni, enti locali)[9] – abbiano una naturale propensione ad agevolare la propagazione di contenuti digitali che dunque tendono a sfuggire al legittimo controllo da parte degli interessati. Una simile strutturazione dell'ambiente è suscettibile di spostare l'ago della bilancia a favore della libera circolazione dei contenuti.

[8] Cfr. A. FUMAGALLI, *Bioeconomia e capitalismo cognitivo: verso un nuovo paradigma di accumulazione*, Roma, Carocci, 2007; C. VERCELLONE, *Capitalismo cognitivo. Conoscenza e finanza nell'epoca postfordista*, Roma, Manifestolibri, 2006. Sul capitalismo delle reti si veda E. RULLANI, *L'economia della conoscenza nel capitalismo delle reti*, in *Sinergie*, n. 76, 2008, 67-90 (v. in particolare, p. 71, 73); V. SANGUIGNI, A. BILOTTA, *Le reti come schema interpretativo per veicolare la conoscenza e governare la complessità*, in *L'industria*, n. 2, 2011, 355-371.

[9] Cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 8/2014 on the recent developments on the internet of things*, 16 september 2014.

Contributi

Il Dossier sanitario elettronico (DSE) tra politiche di e-health ed esigenze di protezione dei dati personali: l'illecito trattamento dei dati personali mediante DSE e l'area del danno risarcibile.

M. Carcione[*]

SOMMARIO: 1. Introduzione. – 2. Le *information and communication technologies* nel sistema sanitario: dalla cartella clinica elettronica al fascicolo sanitario elettronico (FSE) passando per il dossier sanitario elettronico (DSE) – 3. DSE e protezione dei dati personali: le esperienze successive alle linee guida del 2009. – 3.1. I casi: l'Azienda Policlinico Umberto I di Roma, l'Azienda Ospedaliera Universitaria S. Orsola Malpighi di Bologna, l'Azienda Sanitaria della Provincia Autonoma di Bolzano e l'Azienda Ospedaliera Universitaria Ospedali Riuniti di Trieste e di altre aziende sanitarie della regione Friuli Venezia Giulia. – 4. Linee guida sul DSE del giugno 2015: *data breach* e *data protection officer* – 5. L'illecito trattamento dei dati personali mediante DSE e l'area del danno risarcibile. – 6. Conclusioni.

1. Introduzione.

La privacy – intesa come gestione dei propri dati personali e come capacità di mantenere il controllo delle proprie informazioni – rappresenta certamente una delle sfide del prossimo futuro. In una realtà in cui ciascun individuo è sempre più "connesso" – non solo con altre persone ma anche con la rete e con gli oggetti – il continuo sviluppo delle tecnologie pone a rischio in modo sempre più pressante il bisogno di protezione dei dati personali. La tutela della privacy rappresenta, pertanto, sicuramente il banco di prova sul quale si esercitano le nuove esigenze di protezione dell'individuo e pone un

[*] Avvocato in Roma, Studio legale MC LAWYERS; Federprivacy.

problema serio di bilanciamento con altri diritti, primi tra tutti le libertà di espressione e di iniziativa economica.

Cloud computing, big data, internet delle cose: ogni nuova tecnologia richiama la necessità di tutela della privacy e pone, di volta in volta, questioni inedite da affrontare. Appare, pertanto, quanto mai opportuno imparare a confrontarsi con il rischio – attuale ed immanente nel sistema di gestione automatizzata di dati – che l'interessato perda il controllo degli stessi e che, al contempo, non sia consapevole del trattamento subito dalle informazioni trattenute e condivise; in altre parole, trattate. Il problema non è solamente quello di individuare misure di sicurezza adeguate ed al passo con i tempi – che rendano effettivo il controllo dei dati personali e delle informazioni – ma è anche quello di apprestare all'interessato, qualora vi sia stato un illecito trattamento di dati personali, rimedi appropriati, tanto più quando l'illecito trattamento dei dati afferisce ai c.d. dati sensibili, cioè a quei "*dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*"[10].

La tutela dei dati idonei a rivelare lo stato di salute (ma non solo) assume, evidentemente, un rilievo particolare in ambito sanitario, tanto più in un'epoca, quale quella attuale, in cui le Information and Communications Technologies, in acronimo ICT – cioè l'utilizzo di metodi e di tecnologie digitali che realizzano sistemi di trasmissione, ricezione ed elaborazione di informazioni – hanno consentito lo sviluppo della c.d. "sanità digitale" e della "salute in rete" (in inglese e-health). Può, dunque, realisticamente ipotizzarsi che, nell'ambito del *genus* della responsabilità civile da trattamento illecito di dati personali la *species* costituita dalla responsabilità da illecito trattamento di dati sensibili in ambito sanitario (responsabilità

10 Cfr. art. 4, lett. d, del D.Lgs. del 30/06/2003 n. 196 ("Codice della Privacy"), in G.U. 29/07/2003.

extracontrattuale[11] ma, forse, anche contrattuale[12] [13]), attraverso sistemi informatici, costituirà la nuova frontiera del danno risarcibile

[11] La responsabilità extracontrattuale è definita anche aquiliana: essa ricorre in caso di violazione del principio del *neminem laedere*. Cfr. art. 2043 c.c.: "*qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno*".

[12] Essa ricorre quando l'illecito è compiuto nell'ambito di un rapporto obbligatorio contrattuale, genericamente o specificamente disciplinato dalla legge. Cfr. art. 1173 c.c.

[13] Infatti, l'illecito trattamento dei dati non può escludere, *a priori*, anche un inadempimento contrattuale. V. *infra sub* par. 5. E' pacifico che con la richiesta del paziente (ricovero e prestazione medica) insorge, infatti, un rapporto giuridicamente rilevante di natura contrattuale, generatore di diritti soggettivi e di correlativi doveri a carico dell'ente e del suo personale sanitario. Il più complesso rapporto che viene ad instaurarsi con la struttura è stato definito "contratto di spedalità". Invero, "*la responsabilità della casa di cura (o dell'ente) nei confronti del paziente ha natura contrattuale e può conseguire, ai sensi dell'art. 1218 c.c., all'inadempimento delle obbligazioni direttamente a suo carico nonché, ai sensi dell'art. 1228 c.c., all'inadempimento della prestazione medico-professionale svolta direttamente dal sanitario, quale suo ausiliario necessario pur in assenza di un rapporto di lavoro subordinato, comunque sussistendo un collegamento tra la prestazione da costui effettuata e la sua organizzazione aziendale, non rilevando in contrario al riguardo la circostanza che il sanitario risulti essere anche "di fiducia" dello stesso paziente, o comunque dal medesimo scelto*" (*ex multis*: Cass. 14.06.2007, n. 13953; Cass. 14.7.2004, n. 13066; Cass. 26.1.2006, n. 1698; Cass. Sezioni Unite 1.07.2002, n. 9556). Ciò posto, *mutatis mutandis*, nonostante il richiamo operato dall'art. 15 del codice *privacy* all'art. 2050 c.c., nulla osta a che, in determinati casi ed a determinate condizioni, nell'ambito della c.d. responsabilità sanitaria possa essere, in via analogica, sussunta (oltre alla *malpractice* medica ed alla responsabilità derivante da omessa o insufficiente informazione sulla prestazione medica da effettuare, c.d. omesso o insufficiente consenso informato) anche la responsabilità da illecito trattamento di dati attraverso sistemi informatizzati (ma non solo), quali cartelle cliniche elettroniche o *dossier* sanitari elettronici, talché il titolare del trattamento, in caso di illecito trattamento di dati sanitari, possa essere chiamato a rispondere *ex* art. 1218 e ss c.c. per fatto proprio ovvero *ex* art. 1228 c.c. per fatto del responsabile del trattamento (o dei responsabili) nei confronti del paziente/interessato, in solido tra loro. È da ritenersi, infatti, che entrambi siano, potenzialmente, legittimati passivi, dunque, obbligati in solido *ex* art. 2055 c.c. nonché *ex* art. 29, comma 5, codice della *privacy* in forza del quale "*il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare, il quale anche in base a verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni*"). In relazione alla responsabilità da *malpractice* medica cfr. Cass. Sezioni Unite, 11 gennaio 2008, n.

del ventunesimo secolo? Le linee guida del 2015 dell'Autorità Garante sul dossier sanitario elettronico (DSE) – in particolare la previsione dell'obbligo di comunicazione di *data breach*[14] – nonché la proposta di regolamento europeo[15] rendono lo scenario tratteggiato altamente probabile. Da qui la necessità di scandagliare l'area del danno risarcibile in tema di trattamento illecito di dati sensibili in ambito sanitario – in particolare quello effettuato tramite DSE – onde evitare che il rimedio risarcitorio alla lesione della privacy, definita come il "*diritto soggettivo di costruire liberamente e difendere la propria sfera privata*"[16], assuma valenza sanzionatoria, trasformandolo in uno strumento di corresponsione del c.d. danno punitivo, avente scopo preventivo e non ripristinatorio. Tanto più, in ragione del fatto che il concetto di privacy risulta ormai molto più esteso del concetto di riservatezza, inteso come diritto all'intimità privata: nella c.d. "società dell'informazione" i confini del diritto alla privacy tendono, infatti, ad ampliarsi[17].

577: il medico e l'ospedale (senza alcuna differenza tra strutture pubbliche e private) rispondono a titolo contrattuale dei danni arrecati dal sanitario per il solo fatto del "contatto" intervenuto con il paziente, indipendentemente dall'assunzione formale di obblighi riconducibili ad una fonte negoziale tipica. Naturalmente la eventuale responsabilità contrattuale di titolare e/o responsabile del trattamento non escluderebbe la concorrente responsabilità da fatto illecito (anche conseguente a reato) *ex* art. 15 del codice della *privacy* e 2050 c.c. . D'altro canto, l'espresso riferimento operato dal legislatore del 2003 a tale ultimo articolo non varrebbe ad escludere una responsabilità di natura contrattuale di titolare e/o responsabile del trattamento laddove l'illecito trattamento di dati si inserisca - e ne costituisca una declinazione naturale – in un rapporto di tipo negoziale come il c.d. contratto di spedalità ovvero costituisca, quantomeno, un obbligo accessorio alla prestazione principale (quella medica).

[14] Art. 7. 1. *Linee guida in materia di dossier sanitario.* V. *infra sub* 20 e 60.

[15] Cfr. *Proposta di regolamento 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 (regolamento generale sulla protezione dei dati)*, testo proposto dalla Presidenza al Consiglio dell'Unione europea, 11 giugno 2015.

[16] Cfr. S. RODOTÀ, *Repertorio di fine secolo (la costruzione della sfera privata*), Laterza, Bari, 1999, pp. 202 e ss.

[17] Cfr. S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Bari, 1997, pp. 151 e ss.

Tali considerazioni valgono a fortiori in ambito sanitario dove, tradizionalmente, la sensibilità individuale, in ragione della natura dei dati trattati, è indubbiamente maggiore.

2. Le *information and communication technologies* nel sistema sanitario: dalla cartella clinica elettronica al fascicolo sanitario elettronico (FSE) passando per il dossier sanitario elettronico (DSE).

La sanità elettronica "*consiste nell'insieme delle iniziative volte ad archiviare, mediante nuove modalità indotte dall'evoluzione tecnologica, la documentazione che gli enti sanitari utilizzano nei processi di cura dei pazienti*"[18] e si distingue dalla telemedicina il cui ambito è maggiormente circoscritto, posto che essa evoca la "*prestazione di servizi di assistenza sanitaria, tramite il ricorso alle TIC, in situazioni in cui il professionista della salute e il paziente (o due professionisti) non si trovano nella stessa località. Essa comporta la trasmissione sicura di informazioni e dati di carattere medico grazie a testi, suoni immagini o altre forme necessarie per la prevenzione, la diagnosi, il trattamento e il successivo controllo dei pazienti*"[19].

Il legislatore italiano, negli ultimi anni, è più volte intervenuto sul tema della sanità digitale. Basti pensare al decreto legge n. 158/2012[20], convertito con modificazioni dalla legge n. 189/2012[21], al decreto legge n. 179/2012[22] (c.d. "decreto crescita 2.0"), convertito con modificazioni dalla legge n. 221/2012[23], e – da ultimo – al decreto

[18] Cfr. D. SICLARI, *La sanità digitale: profili giuridici e di law and economics*, in *Amministrazione e contabilità dello Stato e degli enti pubblici* (http://www.contabilita-pubblica.it/), 16 febbraio 2013; P. GUARDA, *Fascicolo sanitario elettronico e protezione dei dati personali*, Trento, Università degli Studi di Trento (Ed.), 2011.
[19] Vedi *supra sub* 9.
[20] In GU, Serie Generale, n.214 del 13-9-2012.
[21] In S.O. n. 201, relativo alla G.U. 10/11/2012, n. 263.
[22] In S.O. n. 194, relativo alla GU del 19/10/2012 n.245.
[23] In S.O. n. 208, relativo alla G.U. 18/12/2012, n. 294.

legge n. 69/2013[24] (c.d. "decreto del fare"), convertito con modificazioni dalla legge n. 98/2013[25]. Infine, è intervenuto con il Regolamento in materia di Fascicolo Sanitario Elettronico (FSE)[26]. Prima di questi contributi mancavano, però, *in subjecta materia* fonti normative: gli unici riferimenti erano contenuti nelle linee guida del Ministero della salute e nelle linee guida del Garante per la protezione dei dati personali in materia di Fascicolo Sanitario Elettronico e di *dossier* sanitario elettronico del 16 luglio 2009[27] nonché nelle linee guida in materia di referti *on line* del 19 novembre 2009[28], ai quali si sono aggiunte, ultimamente, le linee guida dell'Autorità Garante in materia di *dossier* sanitario approvate con deliberazione del 4 giugno 2015[29].

Pur non essendo questa la sede per approfondire lo stato dell'arte del processo di digitalizzazione della sanità[30], è opportuno proporre una panoramica a volo di uccello sulla c.d. sanità digitale per poi approfondire la *vexata quaestio* che le ICT, in generale, e la sanità digitale, in particolare, pongono in tutti quei casi in cui *ex post* si constata che qualcosa non ha funzionato nei sistemi di sicurezza: si tratta, in altre parole, di riempire di contenuto un diritto (quello alla *privacy*) che affonda le sue radici nella costituzione, verificando se, ed in che termini, l'ordinamento ne garantisce l'effettività in sede

[24] In S.O. n. 50 relativo alla GU del 21/6/2013 n.144.

[25] in S.O. n. 63, relativo alla G.U. 20/08/2013, n. 194. Per la disciplina legislativa del FSE si veda *Ripubblicazione del testo del decreto-legge 18 ottobre 2012, n. 179 , coordinato con la legge di conversione 17 dicembre 2012, n. 221 (pubblicato nel supplemento ordinario n. 208/L alla Gazzetta Ufficiale 18 dicembre 2012, n. 294) , recante: «Ulteriori misure urgenti per la crescita del Paese.».*, in *G.U.* n. 9 del 11 gennaio 2013, art. 12.

[26] Cfr. DPCM n. 179 del 29/09/2015 in G.U. dell'11/11/ 2015 n. 263.

[27] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009*, in *G.U.* n. 178 del 3 agosto 2009.

[28] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in tema di referti on line – 19 novembre 2009* in *G.U.* n° 288 del 11/12/2009.

[29] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di dossier sanitario - 4 giugno 2015*, in *G.U.* n. 164 del 17 luglio 2015.

[30] Cfr. U. IZZO, P. GUARDA, *Sanità elettronica, tutela dei dati personali e digital divide generazionale*, Trento Law and Technology Research Group, Research Paper Series, n. 3, 2010.

risarcitoria e/o ripristinatoria dello *status quo ante*. In verità, il presente contributo intende focalizzare la sua attenzione sull'illecito trattamento dei dati personali mediante DSE ed indagare, in tale contesto, l'area del danno risarcibile sulla scorta dell'orientamento espresso dalla Corte di legittimità. Ciò non di meno le problematiche sottese all'illecito trattamento dei dati personali in ambito sanitario appaiono, entro certi limiti, comuni alla cartella clinica digitale, al *dossier* sanitario elettronico (DSE) ed al fascicolo sanitario elettronico (FSE). Tanto rilevato – pur avendo, ripetesi, il presente contributo ad oggetto le linee guida dell'Autorità Garante in materia di *dossier* sanitario elettronico[31] con riferimento all'area del danno risarcibile – nel ristretto ambito indicato, vale la pena di sottolineare come l'intervenuto decreto legge 158/2012[32] tragga spunto dalla constatazione della necessità ed urgenza di procedere al riassetto dell'organizzazione sanitaria, anche alla luce della contrazione delle risorse finanziarie a disposizione: riorganizzazione finalizzata al conseguimento di un più alto livello di tutela della salute senza, tuttavia, aggiungere molto altro in materia di FSE.

Ben diversa è la portata innovatrice del decreto legge 179/2012. Ed infatti il mentovato decreto legge[33] disciplina, tra l'altro, la trasmissione telematica delle certificazioni di malattia, uno dei punti cardine del percorso di creazione dell'*e-Health*. La successiva sezione IV è, poi, interamente dedicata alla "sanità digitale"[34]. Successivamente è intervenuto il decreto legge 69/2013[35], che, tra l'altro, ha introdotto misure urgenti volte a favorire la realizzazione del FSE. Ebbene, proprio a seguito di questi ultimi provvedimenti si è reso, quindi, necessario il Regolamento, di cui si è detto, che entra nel merito di una più completa ed organica disciplina del FSE non solo da un punto di vista tecnico ma anche giuridico.

---

[31] V. *supra sub* 20.
[32] V. *supra sub* 11.
[33] Art. 7 . V. *supra sub* 13.
[34] Cfr. art. 12 che si occupa del FSE, art. 13 che affronta i temi della prescrizione medica e della cartella clinica digitale e art. 13 *bis* che disciplina la ricetta medica. V. *supra sub* 13.
[35] Cfr. art. 17. V. *supra sub* 6.

Ma cosa si intende per FSE? Il FSE viene definito dall'art. 12 del DL 179/2012[36], richiamato dal Regolamento, come «*l'insieme dei dati e documenti digitali di tipo sanitario e socio sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito*». Tuttavia, già il Garante per la protezione dei dati personali aveva definito lo stesso, nel proprio provvedimento generale del 2009[37], come "*il fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale*", distinguendolo dal *dossier* sanitario che, pur riguardando gli stessi dati, è costituito presso un organismo sanitario in qualità di unico titolare del trattamento (si pensi ad una clinica privata o struttura sanitaria pubblica) al cui interno operino più professionisti. Tralasciando altri aspetti – che esulano dall'oggetto del presente contributo – degna di menzione è l'introduzione da parte del Regolamento in materia di FSE del concetto di profilo sanitario sintetico o *patient summary*: esso rappresenta il documento socio-sanitario informatico redatto e aggiornato dal medico di medicina generale o pediatra di elezione, che riassume la storia clinica dell'assistito[38]. Parimenti rilevante è la novità rappresentata dal c.d. taccuino personale[39], che consiste in una sezione riservata del FSE all'interno della quale è permesso all'assistito di inserire dati e documenti personali relativi ai propri percorsi di cura. Tanto rilevato, non v'è dubbio che con l'introduzione del FSE nel recente decreto, si è voluto dare una spinta innovativa al paese e un servizio migliore al cittadino, tale da non influenzare certamente l'attività del medico, che continua ad essere l'attore principale del processo.

[36] V. *supra sub* 13.
[37] V. *supra sub* 18.
[38] Cfr. art. 3. Trattasi di un documento che la finalità di favorire la continuità di cura, permettendo un rapido inquadramento dell'assistito al momento di un contatto con il SSN. V. *supra sub* 17. Sull'argomento, si veda anche M. IASELLI, *Fascicolo Sanitario Elettronico: le novità introdotte dal Regolamento*, in *Forum P. A.*, 23 novembre 2015, reperibile all'indirizzo <http://www.forumpa.it/sanita-le-novita-del-regolamento-per-il-fascicolo-sanitario-elettronico>.
[39] Cfr. art. 4. V. *supra su* 17.

Nel concludere questa breve panoramica, corre l'obbligo di definire i rapporti intercorrenti tra cartella clinica elettronica, *dossier* sanitario elettronico e fascicolo sanitario elettronico. Ebbene, la prima[40], viene intesa come atto pubblico – come tale munito di fede privilegiata[41] – e come complesso ordinato di documenti clinici raccolti dai sanitari nel corso di un ricovero, di un *day hospital* o di un *day surgery*. Il FSE, invece, come accennato, è formato con riferimento a dati sanitari originati da diversi titolari del trattamento. Il FSE rappresenta, quindi, una vera e propria carta d'identità sanitaria del singolo cittadino. E' proprio questa ultima considerazione che permette di evidenziarne le differenze con la cartella clinica elettronica (oltre che con il *dossier* sanitario elettronico) perché mentre quest'ultima è interna alla sola struttura ospedaliera ed è riferibile ad un singolo evento clinico – a differenza del *dossier* sanitario che pur essendo riconducibile ad un unico titolare del trattamento contempla più eventi clinici – il FSE è disponibile su tutto il territorio, sempre sulla base del consenso libero e informato da parte dell'assistito (stante il diritto in capo a quest'ultimo di richiedere l'oscuramento dei dati e documenti sanitari e socio-sanitari sia prima dell'alimentazione del FSE che successivamente, garantendone la consultabilità esclusivamente all'assistito e ai titolari che li hanno generati). Probabilmente ancora non si è in grado di valutare la rivoluzione organizzativa che porterà questo strumento: infatti, la gestione dei dati sensibili a livello elettronico crescerà in maniera esponenziale e di pari passo dovranno crescere le misure di sicurezza, le misure organizzative e la tutela dei dati. Conclusivamente, la gestione del FSE – ma lo stesso può certamente dirsi per il DSE e, entro certo limiti, per la cartella clinica elettronica – rientra nel processo più ampio della gestione del dato. Occorre, dunque, essere preparati ad affrontare questa nuova sfida che parte sicuramente dalla formazione e dalla cultura di persone di fatto ancora "analogiche" per passare alla sicurezza intrinseca del dato

[40] Cfr. A. TUZZA, *Il diritto di accesso agli atti degli enti del servizio sanitario nazionale ed il rapporto con la tutela della privacy*, in F. CASTIELLO, V. TENORE (a cura di), *Manuale di diritto sanitario*, Milano, Giuffré, 2012, 521-566.

[41] Cfr. art. 2700 c.c.: essa fa fede fino a querela di falso "*della provenienza del documento dal pubblico ufficiale che lo ha formato, nonché della dichiarazione delle parti o degli altri fatti che il pubblico attesta avvenuti in sua presenza".*

(*privacy by default*) sino a giungere alla piena tutela del dato personale perché ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano: al centro c'è sempre l'uomo (il paziente) e la sua dignità con la quale non ci si può non confrontare. Il problema che ci investe – giova ribadirlo – è culturale prima ancora che normativo: "l'uomo analogico" non è ancora formato, purtroppo, alla tutela della riservatezza personale, tanto più quando il trattamento del dato personale avviene in modo digitale e, quindi, dematerializzato. Quando si tratta di operare un bilanciamento tra interessi di rango costituzionale – che può essere risolto necessariamente sulla scorta di una valutazione comparativa degli interessi in gioco applicando il criterio della prevalenza – spesso si constata che alla tutela del dato personale, in quanto tale, viene attribuito (dalle istituzioni, beninteso, ma non certo dagli interessati!) carattere recessivo…rispetto ad altri interessi di rango costituzionale.

Questa premessa riguardante la cartella clinica elettronica ed il fascicolo sanitario elettronico si è resa necessaria per il fatto che, da una parte, il *dossier* sanitario elettronico (DSE) rappresenta null'altro che una evoluzione della cartella clinica elettronica, dall'altra, in ragione del fatto che il DSE rappresenta un caso particolare (*rectius*, unidimensionale) del FSE, dal quale mutua regole molteplici.

3. DSE e protezione dei dati personali: le esperienze successive alle linee guida del 2009.

Si è accennato al fatto che il *dossier* sanitario elettronico è costituito presso un organismo sanitario in qualità di unico titolare del trattamento, al cui interno operano più professionisti, ed al fatto che si distingue dal fascicolo sanitario elettronico perché, ripetesi, in quest'ultimo confluisce l'intera storia clinica di una persona e coinvolge più titolari di trattamento dati. Ma venendo al *punctum pruriens* della questione, viene alla ribalta una domanda: perché l'Autorità garante, che già era intervenuta con un provvedimento del 16 luglio 2009[42] dedicato (anche ma non solo) al *dossier* sanitario

[42] V. *supra sub* 18.

elettronico, ha avvertito la necessità di tornare in *subjecta materia* con le linee guida del 2015[43], destinate, questa volta, non a caso, esclusivamente al *dossier* sanitario elettronico? Si potrebbe pensare che il Garante per la protezione dei dati personali abbia ritenuto opportuno rendere disponibile un quadro unitario di misure e accorgimenti per conformare i trattamenti di dati personali - e, in particolare, quelli idonei a rivelare lo stato di salute - alla vigente disciplina sulla protezione dei dati personali che tenesse conto dell'esperienza maturata e dell'evoluzione normativa rispetto alle "Linee guida in tema di Fascicolo sanitario elettronico e di *dossier* sanitario" adottate dalla stessa Autorità nel 2009. E ciò sicuramente è vero. Ma la necessità di tale intervento appare ancor più chiara passando in rassegna la "premessa" di cui all'allegato A alla deliberazione del Garante del 4 giugno 2015[44]. Ivi si legge che "l*a sfida che tutti gli attori istituzionali sia nazionali che locali si pongono è, dunque, quella di garantire che i processi di integrazione dei dati sanitari assicurino un buon funzionamento dei sistemi clinici sia in termini di efficacia che di efficienza ed equità nel rispetto dei diritti fondamentali dell'individuo tra i quali si annovera quello alla tutela dei dati personali".* Dunque, il corretto funzionamento dei sistemi clinici deve necessariamente contemperarsi con l'imprescindibile tutela dei diritti individuali, tra i quali primeggia quello alla tutela dei dati personali.

Purtroppo l'esperienza successiva al 2009 ha tradito le aspettative per varie ragioni che il Garante ha evidenziato in modo esemplare[45]. Per un verso – rileva il Garante – "*affinché i dossier sanitari in uso presso le strutture sanitarie siano effettivamente degli strumenti di ausilio nei processi di diagnosi e cura dei pazienti è necessario che gli stessi siano realizzati con modalità tali da garantire in primo luogo la certezza dell'origine e della correttezza dei dati e l'accessibilità degli stessi solo da parte di soggetti legittimati*"; per altro verso – prosegue il Garante – "*la maggior parte dei dossier sanitari esaminati*

[43] V. *supra sub* 20.
[44] V. *supra sub* 20.
[45] Premessa di cui all'allegato A alla deliberazione del Garante del 4 giugno 2015. V. *supra sub* 20.

…omissis…sono stati sviluppati in modo non strutturale e organizzato, bensì partendo da alcune iniziative estemporanee di informatizzazione delle cartelle cliniche di reparto o di ambulatorio e, quindi, senza tener conto del fatto che si andava predisponendo un sistema informativo in grado di gestire potenzialmente l'intera storia clinica di un individuo"[46]. Quale è stato il risultato di tale *modus operandi*? Non solo accessi abusivi ai *dossier* sanitari (consultazione, estrazione, copia delle informazioni sanitarie accessibili tramite il *dossier* da parte di personale amministrativo o personale medico che non era stato mai coinvolto nel processo di cura del paziente e che per motivi di interesse personale aveva acceduto allo stesso per poi divulgare le informazioni così acquisite a terzi all'insaputa dell'interessato (*sic !*) ma, quel che è più grave, nella maggior parte dei casi sottoposti all'attenzione dell'Autorità - intervenuta a seguito di segnalazioni pervenutele - l'accesso aveva riguardato addirittura informazioni relative a prestazioni sanitarie particolarmente delicate alle quali l'ordinamento dedica specifiche disposizioni a tutela della riservatezza e della dignità dei soggetti interessati (ad es., affezioni da HIV, interruzione volontaria della gravidanza, *etc.*)

Alcuni esempi chiariranno la portata del problema sotteso all'intervento del Garante nel 2015 con le mentovate linee guida sul dossier sanitario elettronico[47].

3.1. I casi: l'Azienda Policlinico Umberto I di Roma, l'Azienda Ospedaliera Universitaria S. Orsola Malpighi di Bologna, l'Azienda Sanitaria della Provincia Autonoma di Bolzano e l'Azienda Ospedaliera Universitaria Ospedali Riuniti di Trieste e di altre aziende sanitarie della regione Friuli Venezia Giulia.

Un caso emblematico sottoposto all'attenzione del Garante è stato quello relativo all'Azienda Policlinico Umberto I di Roma[48]. Nella

[46] V. *supra sub* 37.
[47] V. *supra sub* 18.
[48] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Illeicità nel trattamento di dati personali e sensibili presso una struttura ospedaliera - 18 dicembre 2014*, reperibile all'indirizzo http://www.garante privacy.it/web/guest/home/docweb/-

circostanza, erano pervenute all'Autorità Garante alcune segnalazioni nelle quali si lamentava una presunta violazione della disciplina in materia di protezione dei dati personali relativamente alle modalità di funzionamento del sistema informativo di archiviazione e refertazione delle prestazioni sanitarie erogate dall'Azienda Policlinico Umberto I di Roma. In particolare, si lamentava che gli applicativi in uso presso i diversi dipartimenti del Policlinico sarebbero stati configurati in modo tale da consentire a ogni medico di accedere non solo ai dati personali dei propri pazienti, ma anche a quelli di qualsiasi altra persona che sia stata in cura presso la struttura sanitaria. Inoltre, alcuni segnalanti lamentavano di non aver prestato alcun consenso informato in relazione al suddetto trattamento di dati personali. In particolare, in una segnalazione si rilevava che nel predetto sistema informativo sarebbero trattate anche informazioni relative allo stato di sieropositività, senza che il paziente avesse espresso uno specifico consenso al riguardo. Durante le suddette verifiche ispettive *in loco* veniva constatato come il personale sanitario di dipartimento potesse accedere al *dossier* aziendale con riferimento: a) ai pazienti ricoverati in reparto (ovvero dimessi da meno di trenta giorni); b) allo storico degli esami radiologici e di laboratorio nonché allo storico dei rapporti di pronto soccorso; c) ai pazienti non ricoverati in reparto (ovvero dimessi da più di trenta giorni): solo le anagrafiche di accettazione. Peraltro, all'esito della verifica, emergeva la mancanza di specifiche procedure per la gestione di eventuali richieste di oscuramento, venendo tali richieste gestite caso per caso, come pure di sistemi di *audit* automatizzato per il rilevamento di eventuali anomalie negli accessi al *database*.

Ed ancora. Dagli accertamenti ispettivi, risultava come fossero in uso presso i vari dipartimenti modelli di informativa e consenso al trattamento dei dati personali che solo in taluni casi rendevano edotto il paziente circa la possibilità che fossero raccolti – con modalità informatiche – i dati sanitari riferibili alla sua storia clinica precedente; come mancasse la designazione, quali incaricati del

/docweb-display/docweb/3725976, provvedimento n. 610 del 18 dicembre 2014, [doc. web n. 3725976].

trattamento[49], del personale medico ed infermieristico ivi operante. Ebbene, con il provvedimento in esame[50], l'Autorità ha avuto modo di ribadire alcuni principi cardine in materia di sicurezza e di trattamento di dati sensibili e, segnatamente: a) il trattamento dei dati personali effettuato mediante il *dossie*r deve uniformarsi al principio di autodeterminazione[51]; b) pertanto, all'interessato deve essere consentito di scegliere, in piena libertà, se far costituire o meno un *dossier* sanitario con le informazioni cliniche che lo riguardano; c) il consenso, anche se manifestato unitamente a quello previsto per il trattamento dei dati a fini di cura, deve essere autonomo e specifico[52] ; d) il trattamento dei dati sanitari effettuato tramite il *dossier* costituisce un trattamento ulteriore e – come tale – facoltativo rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico per il quale l'interessato si rivolge ad esso; e) in assenza del *dossier* sanitario, infatti, il professionista avrebbe accesso alle sole informazioni fornite dal paziente e a quelle elaborate in relazione all'evento clinico per il quale il paziente si è recato presso di lui; f) il titolare del trattamento deve fornire previamente un'idonea informativa[53]; g) il titolare deve

[49] Cfr. art. 30 e allegato B) del "Codice della Privacy", D.Lgs. del 30/06/2003 n° 196. V. *supra sub* 1.

[50] Cfr. provvedimento n. 610 del 18 dicembre 2014, [doc. web n. 3725976]. V. *supra sub* 40.

[51] Cfr. artt. 75 e ss. del Codice Codice della Privacy", D.Lgs. del 30/06/2003 n° 196, in G.U. 29/07/2003. V. *supra sub* 1.

[52] cfr. artt. 23, comma 3, e 81 del Codice Codice della Privacy, D.Lgs. del 30/06/2003 n° 196, in G.U. 29/07/2003. V. *supra sub* 1.

[53] Cfr. artt. 13, 79 e 80 Codice della Privacy, D.Lgs. del 30/06/2003 n° 196, in G.U. 29/07/2003. V. *supra sub* 1. L'informativa deve contenere tutti gli elementi richiesti dall'art. 13 del Codice. In particolare, deve essere evidenziata l'intenzione di costituire un *dossier* sanitario che documenti la storia clinica dell'interessato per migliorare il suo processo di cura (cfr. art. 76, comma 1, lett. a) del Codice). Deve essere illustrato all'interessato, infatti, che tale strumento, una volta che sia stato costituito con il suo consenso, potrà essere utilizzato da tutti i professionisti che lo prenderanno in cura all'interno della struttura sanitaria, al fine di valutare in modo più completo il suo stato di salute. Tale strumento potrà essere, infatti, consultato nella sua interezza da parte di tutto il personale sanitario che fornirà nel tempo assistenza allo stesso. L'interessato deve essere, poi, informato che l'eventuale

rendere note all'interessato anche le modalità attraverso le quali rivolgersi allo stesso per esercitare i diritti di cui agli artt. 7 e ss. del Codice della *Privacy*, come pure quelle per revocare il consenso espresso in merito alla costituzione del *dossier* o per esercitare la facoltà di oscurare alcuni eventi clinici che lo riguardano); h) in caso di revoca del consenso (liberamente manifestabile in qualsiasi momento), il *dossier* non deve essere ulteriormente alimentato[54]; i) l'inserimento delle informazioni relative ad eventi sanitari pregressi all'istituzione del *dossier* deve, inoltre, fondarsi sul consenso specifico ed informato dell'interessato; l) qualora nel *dossier* siano inserite anche informazioni relative a prestazioni sanitarie offerte a soggetti nei cui confronti l'ordinamento vigente ha posto specifiche disposizioni a tutela della loro riservatezza e dignità personale, il titolare del trattamento deve acquisire una specifica manifestazione di volontà dell'interessato, il quale potrebbe anche legittimamente richiedere che tali informazioni siano consultabili solo da parte di alcuni soggetti dallo stesso individuati; m) l'informativa deve, infine, distinguere – nell'ambito delle finalità perseguite – quelle di cura della salute dell'interessato da quelle amministrative correlate alla cura, poiché solo per il perseguimento delle prime è necessario acquisire il consenso dell'interessato[55].

---

mancato consenso alla costituzione del dossier non incide sulla possibilità di accedere alle cure mediche richieste.

[54] In tal caso i documenti sanitari presenti restano disponibili al professionista o alla struttura interna al titolare che li ha raccolti od elaborati (es. informazioni relative a un ricovero utilizzabili solo dal reparto/dipartimento di degenza) e per eventuali conservazioni per obbligo di legge (cfr. art. 22, comma 5, del Codice), ma non saranno più condivisi da parte degli altri professionisti degli altri reparti/dipartimenti che prenderanno in cura l'interessato.

[55] Cfr. art. 76 e ss. del Codice Codice della Privacy, D.Lgs. del 30/06/2003 n. 196, in G.U. 29/07/2003. V. *supra sub* 1. Il trattamento di dati sensibili per finalità di carattere amministrativo correlate alla cura deve avvenire, infatti, in conformità allo schema tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e delle province autonome, delle aziende sanitarie, degli enti e agenzie regionali/provinciali nonché degli enti vigilati dalle regioni e dalle province autonome, adottato dalla Conferenza delle regioni e delle province autonome su cui il Garante ha espresso parere favorevole (cfr. Provv. 13 aprile 2006, consultabile sul sito www.garanteprivacy.it, doc. web n. 1272225). Successivamente, il Garante ha reso parere favorevole su una versione aggiornata

Altro esempio significativo delle criticità emerse in tema di *dossier* sanitario elettronico prima dell'emanazione delle linee guida in materia di *dossier* sanitario elettronico del giugno 2015 è rappresentato dal caso dell'Azienda Ospedaliera Universitaria S. Orsola Malpighi di Bologna[56]. Anche questa vicenda trae origine da segnalazioni ricevute dall'Autorità Garante concernenti il sistema informativo di archiviazione e refertazione delle prestazioni sanitarie erogate dall'Azienda Ospedaliero Universitaria S. Orsola Malpighi di Bologna, a seguito di un accertamento ispettivo effettuato presso di essa. Segnatamente, si lamentava una presunta violazione della disciplina in materia di protezione dei dati personali con riferimento alle modalità di funzionamento del sistema informativo di archiviazione e refertazione delle prestazioni sanitarie erogate dall'Azienda Ospedaliero Universitaria S. Orsola Malpighi di Bologna. In particolare, si rilevava che l'applicativo in uso presso i diversi dipartimenti dell'Azienda sarebbe stato configurato in modo tale da consentire a ogni medico di accedere non solo ai referti dei propri pazienti, ma anche a quelli di qualsiasi altra persona che avesse effettuato un esame clinico presso la struttura sanitaria. L'accesso del personale sanitario autorizzato sarebbe stato, pertanto, indipendente dalla circostanza che le informazioni che questi potevano conoscere fossero riferite a soggetti diversi dagli stessi assistiti. Ebbene, analogamente a quanto accaduto con riferimento all'Azienda Policlinico Umberto I di Roma, anche nel corso di tale accertamento ispettivo, veniva verificata la riconducibilità al concetto di *dossier* sanitario dello strumento di raccolta e di gestione dei dati dei pazienti utilizzato dalla suddetta Azienda senza l'acquisizione di un consenso specifico in riferimento al *dossier* sanitario e senza la previsione di specifiche procedure informatiche che consentissero al solo personale

del predetto schema tipo di regolamento in relazione alla necessità, evidenziata da parte di più enti, di adeguare i regolamenti regionali sul trattamento dei dati sensibili e giudiziari al mutato quadro normativo (cfr. Provv. del Garante del 26 luglio 2012 doc. web n. 1915390).

[56] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Dossier sanitario elettronico e privacy dei pazienti, 23 ottobre 2014, provv .468,* reperibile all'indirizzo <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3570631>.

sanitario coinvolto nel processo di cura del paziente di accedere al relativo *dossier* per il tempo strettamente necessario alla cura: per accedere all'applicativo era, infatti, sufficiente inserire delle credenziali di autenticazione consistenti in un *username* e in una *password*; una volta effettuato l'accesso, l'utente poteva addirittura effettuare delle ricerche attraverso le funzioni "nuova ricerca" e "ricerca paziente" per le quali non era necessario inserire il nome e il cognome del paziente ed era in condizione di consultare, attraverso il *dossier*, anche informazioni relative ad aspetti molto delicati della sfera privata dell'individuo, quali, ad esempio, quelle connesse agli accertamenti sullo stato di sieropositività, sull'uso di sostanze stupefacenti, *etc*. Appare *ictu oculi* come anche l'Azienda Ospedaliera di Bologna non avesse adottato un quadro di cautele adeguate, al fine di delineare specifiche garanzie e responsabilità nonché misure ed accorgimenti necessari ed opportuni che le strutture sanitarie devono porre a tutela dei pazienti, in relazione ai trattamenti di dati sanitari che li riguardano effettuati mediante i *dossier* sanitari.

Caso ancora più eclatante di trattamento illecito di dati personali è quello relativo all'Azienda sanitaria della provincia autonoma di Bolzano[57]. Anche in questo caso l'*input* della verifica ispettiva è stata una segnalazione, ma questa volta della Corte dei Conti – Procura regionale – Sezione giurisdizionale per il Trentino Alto Adige, con la quale si evidenziava quanto disposto con sentenza irrevocabile della Corte di Appello di Bolzano nei confronti di una dipendente dell'azienda sanitaria dell'Alto Adige, la quale era stata condannata per il reato di cui all'art. 326 del codice penale, per aver abusato della sua qualità di segretaria del reparto di un ospedale regionale di Bolzano, rivelando – in più occasioni e a più dipendenti – lo stato di sieropositività di una collega. Peraltro, la sentenza *de qua* conferma quanto già rilevato in primo grado in merito alla circostanza che sin dal 2007 "*tutto il personale medico, infermieristico e amministrativo, comprese le segretarie del reparto di YY*" potessero "*accedere con*

[57] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati tramite il dossier sanitario aziendale, 3 luglio 2014*, n. 340, reperibile all'indirizzo < http://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/3325808>.

una propria password ai dati contenenti tutta la storia clinica della paziente". Ed ancora una volta i profili di criticità riconducibili al *dossier* sanitario costituito presso la suddetta azienda ospedaliera erano riferibili all'informativa ed al consenso dell'interessato, all'accesso al *dossier* sanitario ed al diritto dell'interessato a richiedere l'oscuramento di un singolo evento clinico presente nel *dossier* sanitario.

Per concludere questa panoramica, non può sottacersi il caso dell'Azienda Ospedaliera Universitaria Ospedali Riuniti di Trieste e di altre aziende sanitarie della regione Friuli Venezia Giulia[58]. Questa volta la verifica da parte dell'Autorità Garante partiva da una segnalazione anonima nella quale si lamentava come il sistema informativo di archiviazione e refertazione delle prestazioni sanitarie erogate dalle strutture sanitarie della Regione Friuli Venezia Giulia, sarebbe stato strutturato in modo tale da consentire a ogni medico, tramite l'inserimento di uno *username* e di una *password*, di accedere ai referti sia dei propri pazienti sia di qualsiasi altra persona che avesse effettuato un esame clinico presso la struttura sanitaria, a prescindere dal fatto che li avesse in cura o meno. Ancora una volta veniva appurato che il sistema di gestione delle informazioni sanitarie dei pazienti gestito dall'applicativo in uso presso la struttura sanitaria era riconducibile al concetto di *dossier* sanitario e che l'operatore sanitario, utilizzando gli applicativi in uso presso la struttura, aveva non solo la possibilità di accedere alla documentazione clinica relativa a tutti gli episodi medici occorsi ad un paziente all'interno del reparto in cui svolgeva la sua attività professionale, ma, attraverso l'uso di specifiche funzioni presenti in tali applicativi, anche ad un ulteriore applicativo denominato "visualizzatore referti" che consentiva allo stesso di visualizzare l'elenco di tutti gli episodi medici occorsi allo stesso paziente all'interno dell'intera azienda ospedaliera, nonché di tutti i relativi documenti clinici, visualizzando

[58] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Dossier sanitario elettronico e trattamento dei dati personali dei pazienti*, *10 gennaio 2013*, n. 3, reperibile all'indirizzo < http://www.garanteprivacy.it/web/.

persino la documentazione clinica relativa a qualsiasi persona fosse stata in cura, anche in passato.

4. Linee guida sul DSE del giugno 2015: data breach e data protection officer.

Dunque, le criticità rilevate dal Garante attraverso le verifiche ispettive effettuate nelle strutture sanitarie menzionate (tutte su segnalazione), da una parte, e la constatazione che negli ultimi anni le strutture ospedaliere hanno notevolmente incrementato l'utilizzo di sistemi informativi per la gestione della documentazione sanitaria, dall'altra, hanno creato l'*humus* fertile per un nuovo intervento del Garante, il quale, con deliberazione del 4 giugno 2015[59], ha emanato le linee guida dell'Autorità Garante in materia di *dossier* sanitario.

Questa volta, rispetto al 2009, l'attenzione è stata focalizzata esclusivamente sul *dossier* sanitario elettronico e non anche sul fascicolo sanitario elettronico. Il Garante per la protezione dei dati personali ha ritenuto, infatti, opportuno rendere disponibile un quadro unitario di misure tale da conformare i trattamenti di dati personali e, in particolare, quelli idonei a rivelare lo stato di salute, alla vigente disciplina sulla protezione dei dati personali anche alla luce dell'esperienza maturata e dell'evoluzione normativa rispetto alle "Linee guida in tema di Fascicolo sanitario elettronico e di *dossie*r sanitario" adottate dal Garante con provvedimento del 16 luglio 2009 che, evidentemente, non avevano dissipato tutti i dubbi e le incertezze in ordine al trattamento di dati tramite *dossier* sanitario.

Non è possibile in questa sede affrontare *funditus* le novità introdotte dalle suddette linee guida. Un cenno, però, meritano i diritti riconosciuti all'interessato, come la possibilità di richiedere l'oscuramento delle informazioni e/o dei documenti oggetto del *dossier*[60] e la sicurezza dei dati trattati mediante *dossier* sanitario

[59] V. *supra sub* 20.

[60] In questo caso, essi restano comunque disponibili al professionista sanitario o alla struttura interna al titolare che li ha raccolti o elaborati. Il Garante precisa che l'oscuramento dell'evento clinico, revocabile nel tempo, deve avvenire con modalità tali da garantire che i soggetti che sono abilitati all'accesso non possano venire

elettronico. All'uopo, l'Autorità ha inteso indicare le principali misure di sicurezza che il titolare del trattamento dei dati personali deve assicurare[61]. Ma la novità più rilevante è la previsione del c.d. *data breach*. Risulta, infatti, obbligatoria la comunicazione al Garante in caso di eventuali violazioni dei dati (*data breach*) o incidenti informatici (ad es. accessi abusivi, azione di *malwar*e, *etc*.), oppure anche solo nel caso in cui i dati siano stati esposti a rischi di violazione. Entro 48 ore dalla conoscenza del fatto, i titolari del trattamento dei dati sono tenuti a comunicare all'Autorità tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il *dossier* sanitario. Tali comunicazioni devono essere redatte secondo lo schema riportato nell'Allegato B delle Linee guida sul *dossier* sanitario. Sul punto, occorre considerare che la mancata comunicazione al Garante configura un illecito amministrativo, sanzionato ai sensi dell'art. 162, comma 2-*ter* del Codice. E' notorio come la perdita, la distruzione o la diffusione di dati personali possa comportare un grave danno per gli interessati. Si pensi alle conseguenze di truffe informatiche, di furti di identità, di lesioni alla reputazione e alla riservatezza. Per questa ragione, prima il legislatore europeo e poi quello italiano avevano delineato (sia pure per ora solo nel settore delle comunicazioni elettroniche) un quadro giuridico finalizzato a prevenire e gestire il rischio di violazione dei dati che fa

automaticamente a conoscenza del fatto che l'interessato abbia effettuato tale scelta ("oscuramento dell'oscuramento"). Cfr. S. UNGARO, E. MAIO, *Dossier sanitario elettronico: nuove tutele per i pazienti*, in *Agenda digitale EU*, 24 luglio 2015, reperibile all'indirizzo < http://www.agendadigitale.eu/egov/dossier-sanitario-elett ronico-nuove-tutele-per-i-pazienti_1619.htm>.

[61] In particolare, le misure di sicurezza indicate dal Garante possono essere così schematizzate: a) misure a protezione dell'identità del paziente e utilizzazione di canali di comunicazione sicuri; b) adozione di sistemi di autenticazione e autorizzazione che assicurino l'accesso selettivo ai dati in linea con i principi di necessità, pertinenza, non eccedenza e indispensabilità; c) individuazione di criteri e modalità per la separazione e la cifratura dei dati idonei a rivelare lo stato di salute e la vita sessuale degli interessati; d) registrazione delle operazioni di accesso in appositi *file* di *log* ai fini della verifica della liceità del trattamento dei dati; d) realizzazione di procedure per assicurare l'integrità, la disponibilità dei dati e il ripristino degli stessi in caso di guasti, malfunzionamenti o eventi disastrosi.

perno su alcuni obblighi specifici che gravano su particolari titolari del trattamento di dati personali[62]. Non si tratta, quindi, di novità assolute: certamente l'impatto del *data breach notification* e l'espressa previsione del *data protection officer*[63] in ambito sanitario avrà un impatto enorme di cui oggi non si è ancora in grado valutarne a pieno la portata. E' prevista, infatti, non solo la comunicazione di c.d. *data breach* al Garante ma anche all'interessato, al quale il titolare del trattamento, tramite determinate procedure, dovrà rendere note "senza

[62] Cfr. art. 32 *bis* del Codice Privacy che prevede determinati *"adempimenti conseguenti ad una violazione di dati personali"* a carico del "*fornitore di servizi di comunicazione elettronica accessibili al pubblico*" o, per comodità di lettura, del *provider* informatico o telefonico. V. *supra sub* 1.

[63] Cfr. art. 7.1. delle citate linee guide in materia di dossier sanitario elettronico: "*Le peculiari caratteristiche del trattamento dei dati effettuato mediante il dossier sanitario, strettamente connesse alla delicatezza delle informazioni trattate, nonché all'esigenza di garantire l'esattezza, l'integrità e la disponibilità dei dati e la protezione da accessi non autorizzati e da trattamenti non consentiti, rendono necessario assoggettare il loro trattamento…omissis…all'obbligo di comunicazione al Garante del verificarsi di violazioni dei dati (data breach) o incidenti informatici (accessi abusivi, azione di malware…) che, pur non avendo un impatto diretto sui dati stessi, possano comunque esporli a rischi di violazione. A questo fine, si prescrive ai sensi dell'art. 154, comma 1, lett. c), del Codice che, entro quarantotto ore dalla conoscenza del fatto, i titolari comunichino all'Autorità tutte le violazioni dei dati o gli incidenti informatici che possano avere avuto un impatto significativo sui dati personali trattati attraverso il dossier sanitario. Tali comunicazioni devono essere redatte secondo lo schema riportato nell'"Allegato B" al provvedimento del 4 giugno 2015 e inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.dossier@pec.gpdp.it. La mancata comunicazione al Garante delle suddette violazioni o dei predetti incidenti informatici configura un illecito amministrativo sanzionato ai sensi dell'art. 162, comma 2-ter, del Codice. In ragione della particolare delicatezza del trattamento dei dati effettuato mediante il dossier sanitario, l'Autorità ritiene, inoltre, necessario che il titolare individui una procedura per comunicare senza ritardo all'interessato le operazioni di trattamento illecito effettuate dagli incaricati o da chiunque sui dati personali trattati mediante il relativo dossier…omissis…*" mentre l'art. 7.2 delle citate linee guida così dispone: *"…omissis… in ragione della particolare delicatezza delle informazioni trattate mediante il dossier sanitario, il Garante auspica che i titolari del trattamento individuino al loro interno una figura di responsabile della protezione dei dati che svolga il ruolo di referente con il Garante (c.d. DPO - data protection officer), anche in relazione ai casi di data breach…omissis…".*V. *supra sub* 13.

ritardo" le operazioni di trattamento illecito effettuate non solo dagli incaricati, ma da chiunque!

Quale possa essere la ricaduta di tale obbligo (soprattutto della comunicazione all'interessato) è agevole intuirlo: come accennato in premessa, non è azzardato immaginare come la tutela della *privacy* individuale – beninteso in senso formale e non sostanziale - possa in un futuro non tanto lontano costituire la nuova frontiera del danno risarcibile e prestarsi ad intenti biecamente speculativi che poco hanno da spartire con una libertà fondamentale, realizzando quello che non pare esagerato definire come un vero e proprio "assalto alla diligenza".

5. L'illecito trattamento dei dati personali mediante DSE e l'area del danno risarcibile.

L'introduzione delle *information and communication technologies* (ICT) nel sistema sanitario (*e-health*) ha sensibilmente ampliato le capacità cognitive dei medici con il trattamento di dati riguardanti il quadro sanitario degli interessati, in tal modo rafforzando le capacità di prevenzione e i processi di diagnosi e di cura. Tuttavia, tale constatazione non deve far passare in secondo piano la particolare natura dei dati sanitari: il carattere personale e sensibile degli stessi è certamente meritevole di protezione, delineando un diritto fondamentale rispetto al quale, tuttavia, la sanità digitale appare meno permeabile. Ebbene, in questo particolare contesto storico, si pone la seguente questione: da un parte, la sensazione che si trae da alcuni casi riguardanti la gestione del *dossier* sanitario digitale (almeno sino ad oggi) induce a ritenere come la tutela della *privacy* abbia assunto, di fatto e ad onta dei proclami, carattere recessivo rispetto alla tutela della conoscenza, alla circolazione delle informazioni e se, si vuole, alla tutela della salute, intesa come integrità psico-fisica o assenza di patologie (piuttosto che come stato di benessere in senso lato); dall'altra, l'intervento del Garante con le linee guida in materia di *dossier* sanitario elettronico del giugno 2015 – in particolare con l'introduzione degli obblighi di comunicazione di *data breach* (non tanto all'Autorità Garante ma) all'interessato – rischiano di scatenare

quello che, in modo naturalmente provocatorio, è stato definito "assalto alla diligenza", aprendo il varco a richieste risarcitorie bagatellari, avanzate da chi, sotto l'egida di una tutela (solo formale) della *privacy*, è mosso da fini meramente speculatori, da realizzare inserendosi tra le maglie di un sistema di gestione informatizzata di dati sensibili tramite DSE (ma, ovviamente, lo stesse potrebbe dirsi per il FSE) che, ad oggi, non appare ancora pronto per la rivoluzione digitale.

Non è fantascienza, come anticipato, immaginare a breve una esplosione (o, se si vuole, estensione) del contenzioso afferente l'area della responsabilità sanitaria[64], tale per cui l'attuale sistema per così dire "a doppio binario" [per semplificare, responsabilità da *malpractice* medica e/o da omessa o insufficiente informativa sulla prestazione medica (c.d. consenso informato)], potrà trasformarsi in un sistema a "triplo binario", implementandosi con le particolari ipotesi di responsabilità da illecito trattamento informatizzato di dati sanitari. In un contesto in cui le richieste di risarcimento nei confronti di medici e strutture sanitarie, negli ultimi 20 anni sono aumentate del 300%[65] - al punto che la c.d medicina difensiva[66] ha assunto proporzioni enormi con tutto quello che ne consegue in termini di costi per la sanità - tanto da rendere non più procrastinabile un intervento finalizzato all'inversione del *trend* , l'attenzione (non già di

[64] In senso lato o atecnico, intendendosi per tale qualsivoglia ipotesi di responsabilità che si manifesta in seno o *a latere* del rapporto, anche di fatto, che si instaura con una struttura sanitaria, pubblica o privata.

[65] Secondo una ricerca condotta dalla Divisione Ricerche Claudio Dematté della SDA Bocconi *School of Management* e sponsorizzata dai principali *broker* internazionali coinvolti nella sanità italiana al fine di "*sviluppare un modello analitico che possa aiutare a delineare i trend emergenti nel rischio e nella gestione del rischio nelle aziende sanitarie italiane a livello regionale*", come riporta la ricerca "*Criteri di analisi e di valutazione delle scelte assicurative nelle aziende sanitarie*", condotta nel 2012-2013. Cfr. articolo, *Malpractice medica: richieste di risarcimento in crescita costante*, reperibile all'indirizzo < http://www.aboutpharma.com/blog/2014/10/09/malpractice-medica-richieste-di-risarcimento-in-crescita-costante/>.

[66] la medicina difensiva consiste nella pratica di trattamenti terapeutici o misure diagnostiche condotti principalmente, non per assicurare la salute del paziente, ma come garanzia da responsabilità medico legali seguenti alle cure mediche prestate.

interessati realmente danneggiati ma) di speculatori potrebbe "deviare" verso il nuovo "*far west"* della *privacy* in ambito sanitario (ma non solo). In altre parole, l'ipotizzato sistema "a tre binari" (*malpractice* – difetto di informativa sulla prestazione – illecito trattamento di dati) potrebbe indurre i "nuovi pionieri", animati dalla speranza di monetizzare quanto più possibile, a gettare le reti a strascico nella speranza che, *hinc et hinde*, qualcosa vi rimanga impigliato. Appare, dunque, quanto mai opportuno inquadrare l'area del danno risarcibile da illecito trattamento di dati tramite *dossier* sanitario elettronico (ma considerazioni analoghe valgono, naturalmente, anche per il FSE). Ebbene, la disciplina della responsabilità da illecito trattamento di dati personali è data, nell'ordinamento nazionale, dal combinato disposto dell'art. 15[67] e 11[68] del codice della *privacy* e dell'art. 2050[69] del codice civile; combinato disposto che dispone la risarcibilità del danno qualora i dati personali non vengano trattati in modo lecito o secondo le regole della correttezza, non siano stati raccolti e registrati per scopi determinati, espliciti e legittimi, non siano pertinenti, completi, oppure eccedano le finalità della raccolta. Proprio il rinvio all'art. 11 operato

[67] Cfr. art. 15 del "Codice della Privacy", D.Lgs. del 30/06/2003 n° 196 "*Danni cagionati per effetto del trattamento - Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11*". V. *supra sub* 1.

[68] Cfr. art. 11 del "Codice della Privacy", D.Lgs. del 30/06/2003 n° 196 *"Modalità del trattamento e requisiti dei dati . I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. 2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*". V. *supra sub* 1.

[69] "*Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati (1), è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno*".

dal legislatore ha posto – e pone - problemi interpretativi[70], potendo comportare quella proliferazione del contenzioso per violazione della *privacy* di cui si è accennato, se non correttamente interpretato. Tuttavia, come è stato opportunamente osservato[71], "*l'art. 11 del codice della* privacy *... va considerato come l'architrave su cui verificare l'antigiuridicità della condotta di trattamento dei dati personali, ma non l'ingiustizia del danno, intesa, quest'ultima, come lesione al diritto tutelato dalla normativa di settore, necessaria, qualora il pregiudizio sia serio, a dare ingresso al risarcimento del pregiudizio patito*".

Il diritto fondamentale alla protezione dei dati personali deve essere coniugato, infatti, con gli altri diritti fondamentali ed inviolabili della persona umana e deve essere tutelato in modo funzionale alla realizzazione di un contemperamento tra l'interesse individuale di tutti i consociati a difendere la propria riservatezza e l'interesse, speculare, a conoscere e trattare dati personali altrui, talché dalla semplice circostanza che il legislatore abbia inserito un dato diritto, quale

[70] ma anche il rinvio all'art. 2050 c.c. ha posto e pone tuttora dubbi interpretativi. Infatti, potrebbe ritenersi che il trattamento di dati personali costituisca "attività pericolosa" proprio perché (già prima nell'art. 18 L. 675/96 ed ora) nell'art. 15 d.lgs. 196/03 si fa riferimento all'art. 2050 c.c. che disciplina la responsabilità per l'esercizio di attività pericolose. Secondo tale interpretazione, potrebbe rinvenirsi, dunque, una "pericolosità" *ex se* nel trattamento dei dati personali sia per la natura automatizzata e seriale dell'attività, sia perché i mezzi impiegati, per la loro velocità ed ampiezza nella diffusione, rendono altamente probabile il verificarsi di lesioni a diritti fondamentali della persona, come ad es. il diritto alla riservatezza ed all'identità personale. Cfr. in tal senso S. SICA, *Commento all'art. 29, comma 9*, in AA.VV., *La tutela dei dati personali. Commentario alla l. 675/1996*, Padova, 1997, p. 284 ss.. Secondo altra interpretazione, il trattamento dei dati personali non costituisce attività intrinsecamente pericolosa, talché il riferimento all'art. 2050 c.c., contenuto nell'art.18 della legge sulla *privacy*, non avrebbe alcun valore se non quello di indicare il regime probatorio da seguire (cioè l'inversione dell'onere della prova), in ottemperanza alle stesse disposizioni contenute nella dir. CE 95/46. Tale opinione, a parere di chi scrive, appare preferibile perché inserire il trattamento dati nel novero di quelle attività intrinsecamente pericolose appare eccessivo. E' possibile, infatti, equiparare l'attività di trattamento di dati personali con l'attività di che produce polveri da sparo o bombole di gas liquido o, ancora, con l'attività di un imprenditore chimico o farmaceutico? Cfr in tal senso M. FRANZONI, *Dati personali e responsabilità civile*, in *RCP*, 1998, p. 902.

[71] Cfr. Cass. civile, sez. III , n. 24986 del 25/11/2014.

quello alla riservatezza, nell'alveo del rimedio risarcitorio del danno non patrimoniale, non si può inferire, di per sé, che esso sia, sempre e comunque, risarcibile. Ciò in quanto non è configurabile un danno non patrimoniale *in re ipsa*, anche nel caso di lesione di diritti inviolabili[72]. Il danno, sia esso patrimoniale che non patrimoniale, deve essere, comunque, provato e l'onere della prova (del danno e della sua entità) incombe sull'interessato, nonostante il richiamo operato dall'art. 15 del codice della *privacy* all'art. 2050 del codice civile. Invero, il richiamo a tale articolo comporta esclusivamente un alleggerimento dell'onere della prova rispetto a quanto previsto in ambito di responsabilità aquiliana dall'art. 2043 c.c.: onere del danneggiato sarà, infatti, non solo quello di provare il rapporto di causalità tra fatto e danno (e non anche il dolo o la colpa dell'autore del fatto illecito) ma anche l'entità dello stesso, quanto meno in via presuntiva (tenendo presente che le presunzioni operano sulle allegazioni di parte) mentre incomberà al danneggiante l'onere, ben più impegnativo, di provare di aver posto in essere tutte le misure idonee per evitare l'evento dannoso, non essendo sufficiente dimostrare di non aver violato norme di legge o di prudenza o di perizia. Per misure idonee ad evitare il danno devono intendersi tutti gli accorgimenti previsti da norme legislative o regolamentari che disciplinano la specifica attività interessata dalla controversia: nel caso specifico non solo le norme del Testo Unico, il disciplinare tecnico in materia di misure minime di sicurezza (allegato B), ma anche le prescrizioni impartite dal Garante o i codici di deontologia e di buona condotta. Pertanto, la mera violazione dei principi di cui all'art. 11 del codice della *privacy*, che costituisce pur tuttavia l'architrave del sistema, non è da sola sufficiente a determinare una lesione ingiustificata del diritto alla protezione dei dati personali che, invece, potrà configurarsi solamente quando l'offesa superi in modo sensibile la soglia di tollerabilità. Non

[72] Cfr. Cass. Civ. n. 10527 del 2011 e la n. 22100 del 2013. Per un esame della materia Cfr. G. COMANDÈ, *Commento sub art. 15*, in C.M. BIANCA e F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003 n. 196*, Padova, 2007, 362), R. FOFFA, *Caso Vieri: quanto vale la lesione della privacy*, in *Danno e Responsabilità*, 2013, 51; A. GARIBOTTI, *La quantificazione del danno non patrimoniale da lesione della privacy di un calciatore*, in *Danno e Responsabilità*, 2013, 309).

può essere accolta, infatti, la tesi propugnata da chi sostiene che la lesione di un bene fondamentale della persona, quale la riservatezza, di per sé implica un danno non patrimoniale costituito dal turbamento psichico che il soggetto ha risentito per effetto della violazione, come pure la tesi di chi sostiene che il codice della *privacy* privilegi l'adozione di uno strumento risarcitorio con funzione preventiva, pur non perdendo la propria caratteristica funzione, qualora il singolo danneggiato si avvalga, in concreto, della tutela risarcitoria[73]. Il nostro ordinamento, infatti, subordina il diritto al risarcimento del danno alla prova di un concreto pregiudizio economico[74] mentre è estranea al nostro sistema l'idea della punizione del responsabile civile[75], per cui appare indifferente la valutazione a tal fine della sua condotta[76]: non sono risarcibili i c.d. danni punitivi, in quanto la loro funzione sanzionatoria contrasta con i principi fondamentali dell'ordinamento interno, che assegna alla responsabilità civile una funzione ripristinatoria della sfera patrimoniale del soggetto leso[77].

Tanto rilevato, come la natura del danno conseguente ad una violazione dei diritti della personalità, ed in particolare del diritto alla *privacy*, presenta di frequente una connotazione non patrimoniale, così, in ipotesi di illecito trattamento dei dati personali, il danno subito dall'interessato assumerà probabilmente i caratteri del danno non patrimoniale. Ciò non di meno, non possono escludersi *a priori* pregiudizi che presentano il carattere della patrimonialità. Innanzitutto, un primo tipo di pregiudizio economicamente valutabile

[73] In tal senso, E. LUCCHINI GUASTALLA, *Trattamento dei dati personali e danno alla riservatezza*, in *Resp. civ. e prev.*, 2003, p. 651, V. COLONNA, *Il danno da lesione della privacy*, in *Danno e resp.*, 1998, p. 27, A. DI MAJO, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in AA. VV. *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 237.

[74] Cfr. Cass. n. 15184 del 2008.

[75] Cfr. Cass. n. 1781 del 2012.

[76] Cfr. Cass. n. 1183 del 2007.

[77] Tuttavia, fermo restando il riconoscimento della natura compensativa e non punitiva del nostro sistema di responsabilità civile, negli ultimi anni la Corte di Cassazione aveva, con due significative pronunce, di fatto, aperto uno spiraglio all'affermazione di una funzione anche sanzionatoria dell'istituto del risarcimento dei danni. In tal senso, cfr. Cass. n. 11353 del 2010 e Cass. n. 8730 del 2011.

può essere identificato nel prezzo del consenso al trattamento dei dati personali che l'interessato, ove fosse stato debitamente informato, avrebbe richiesto; quindi, può ipotizzarsi un danno ricollegabile alla difficoltà di proseguire la propria attività lavorativa in conseguenza del discredito prodotto dall'illecito trattamento ovvero alla difficoltà di ricollocarsi nel mondo del lavoro (si pensi alla diffusione di dati sensibili contenuti nei *dossier* sanitari elettronici riferibili a particolari infezioni o patologie discriminanti).

Il danno patrimoniale, tuttavia, potrebbe anche integrare un danno da perdita di *chance*: ad esempio l'interessato, a seguito della diffusione di dati sensibili potrebbe veder diminuire in misura rilevante la possibilità di contrarre un buon matrimonio oppure potrebbe rimanere escluso da determinati ambienti altolocati nei quali avrebbe potuto conoscere persone influenti. Ovviamente il pregiudizio patrimoniale derivante da illecito trattamento dei dati deve essere prima allegato e poi provato; quindi potrà essere risarcito *ex* art. 1223 c.c. *sub specie* di danno emergente e lucro cessante[78]. Ciò posto, il pregiudizio cagionato da illecito trattamento di dati sensibili tramite *dossier* sanitario elettronico, assumerà, come anticipato, prevalentemente il carattere di danno non patrimoniale, la cui categoria generale è stata elaborata dalla giurisprudenza in tema di illecito aquiliano. All'uopo, occorre preliminarmente evidenziare come già la stessa nozione di questo particolare pregiudizio sia tuttora oggetto di un'annosa questione; esso può essere definito come la lesione di interessi inerenti la persona non connotati da rilevanza economica. All'epoca dell'emanazione del codice civile[79] l'unica previsione espressa di risarcimento del danno non patrimoniale era quella contenuta nell'art. 185 c.p., per cui la tradizionale lettura restrittiva dell'art. 2059 c.c., in relazione all'art. 185 c.p., comportava che il danno non patrimoniale, sofferto dalla persona offesa e dagli

[78] L'art. 1223 c.c. così recita: "*il risarcimento del danno per l'inadempimento o per il ritardo deve comprendere così la perdita subita dal creditore come il mancato guadagno, in quanto ne siano conseguenza immediata e diretta*". Il depauperamento del patrimonio del debitore si sostanzia nel c.d. danno emergente mentre il mancato guadagno configura il c.d. lucro cessante. Ovviamente deve sussistere il nesso di causalità tra illecito e danno, mutuata dall'art. 40 c.p.

[79] Approvato con R.D. del 16 marzo 1942, n. 262 in G.U. n.79 del 4/4/1942) .

eventuali ulteriori danneggiati, sarebbe stato ristorabile soltanto nel caso in cui l'illecito avesse configurato un'ipotesi di reato. Questa lettura restrittiva è stata però abbandonata a partire dalle sentenze nn. 8827 e 8828 del 31 maggio 2003 (nonché dalla pronuncia della Corte Costituzionale n. 233 dell'11 luglio 2003) con cui è stata estesa l'area di operatività dell'art. 2059 c.c., ricomprendendovi i danni non patrimoniali derivanti da lesione di diritti costituzionalmente garantiti anche qualora il fatto non avesse integrato gli estremi di un reato. Tale nuova ricostruzione ermeneutica ha avuto rilevanza, altresì, in tema di prova del danno; le c.d. sentenze gemelle del 2003 hanno chiarito, infatti, che non è l'offesa all'interesse di rango costituzionale ad essere *ex se* risarcibile, ma tutte le evenienze lesive che ne conseguono sugli aspetti non patrimoniali della vita del danneggiato (si pensi, oltre al caso in questione di cui all'art. 15 del codice della *privacy*, al mancato rispetto del termine ragionevole di durata del processo *ex* art. 2 legge 89/2001). Questa nuova lettura dell'art. 2059 c.c. è stata confermata dalla Cassazione a Sezioni Unite (Cass. S.U. n. 26972 dell'11 novembre 2008 e Cass. S.U. n. 3677 del 16 febbraio 2009) che ha affermato che il danno non patrimoniale è ristorabile non solo quando la risarcibilità sia espressamente prevista dalla legge, ma anche quando il fatto illecito abbia violato in modo grave i diritti della persona, oggetto di tutela *ex* art. 2 della Costituzione.

Quanto alla natura della responsabilità da illecito trattamento dei dati personali essa ha natura aquiliana[80]: ad essa, però, "*non consegue un'automatica risarcibilità, dovendo il pregiudizio morale o patrimoniale essere comunque provato secondo le regole ordinarie*".[81]. Non può escludersi, pero, a priori, che il fatto illecito integri un inadempimento contrattuale: si pensi ad esempio alla diffusione di dati bancari relativi ad un rapporto di conto corrente in violazione delle condizioni generali relative al rapporto banca/cliente. Non c'è dubbio che l'istituto bancario, salva la responsabilità penale del titolare e /o del responsabile al trattamento dei dati[82], si sia reso inadempiente alle clausole contrattuali e sarà, pertanto, chiamato a

[80] Cfr. Cass. del 03/07/2014 n° 15240.
[81] V. *supra sub* 72.
[82] *Ex* art. 167 codice *privacy*. V. *supra sub*. 1.

rispondere, a titolo di responsabilità contrattuale, ex art. 1218 e 1223 c.c. dei danni patiti dal cliente/interessato, in quanto siano conseguenza immediata e diretta della condotta illecita (integrante, però, anche un inadempimento delle condizioni di contratto) perpetrata dalla banca. La qualificazione della responsabilità da illecito trattamento dei dati come aquiliana o contrattuale non è di poco momento, non tanto in relazione al regime probatorio (atteso il richiamo operato dall'art. 15[83] del Codice della Privacy all'art. 2050 c.c.) quanto, piuttosto, al termine di prescrizione che, nel caso della responsabilità contrattuale, è decennale[84] mentre, in caso di responsabilità extracontrattuale, è quinquennale[85].

6. Conclusioni.

Tirando le fila delle considerazioni svolte, non può considerarsi remota la prospettiva che l'introduzione dell'obbligo di comunicazione (anche all'interessato) di *data breach* con riferimento a *dossier* sanitari elettronici, provochi la proliferazione di azioni giudiziarie finalizzate al risarcimento dei danni, patrimoniali e non, per illecito trattamento dei dati sensibili in ambito sanitario, tanto più se si considera che trattasi di dati che, essendo oggetto di trattamento tramite un *dossier* sanitario elettronico, lasciano presagire che l'interessato sia vittima di una patologia che spesso può avere riflessi rilevanti sulla vita quotidiana, se posti a conoscenza di terzi. A fronte, infatti, dell'orientamento stringente sopra richiamato, ancora oscillante appare la giurisprudenza di legittimità in ordine alla illecita diffusione di dati personali di tipo sensibile. Valga titolo esemplificativo un caso recente. La Corte Suprema – dopo che il giudice di prime cure aveva negato il diritto al risarcimento del danno all'interessato, insegnate in un circolo didattico, che erroneamente aveva trasmesso all'istituto copia integrale del verbale di accertamento della commissione medica al fine della verifica dell'esistenza dei

[83] V. *supra sub*. 1
[84] Cfr. art. 2946 c.c.;
[85] Cfr. art. 2947 c.c..

presupposti per ottenere la pensione di inabilità (dal quale risultata una infezione da HIV) in luogo della parte di interesse esclusivo – ha ritenuto che la violazione della *privacy* sussistesse *in re ipsa*, costituendo il precipitato della violazione delle norme di sicurezza, ad onta di quanto affermato dalla Corte suprema a S.U. nelle famose sentenze di San Martino[86] (ma non solo) secondo le quali il danno non patrimoniale è sempre un danno conseguenza: esso non si identifica con la lesione sia pure di un valore costituzionalmente garantito ma con una perdita che a quella lesione consegue.

Non v'è chi non veda come qualora non si tratterà neppure di errori umani – come nel caso in esame – ma di *data breach* derivanti da supporti informatici che per loro intrinseca natura sono esposti a simili violazioni, un approccio giurisprudenziale come quello appena riportato, potrebbe avere effetti devastanti. Peraltro, onde evitare che si verifichino casi in cui vengono riconosciute somme doppie, se non addirittura triple, rispetto alle cifre che generalmente vengono riconosciute in caso di illecito che abbia provocato la morte della vittima, sarebbe auspicabile un intervento legislativo chiarificatore più che innovatore, tale da fissare dei punti fermi nella materia in esame relativamente all'*an debeatur*, per poi soffermarsi anche sul *quantum*. Si evince, infatti, dalla breve analisi sopra condotta, che le c.d. tabelle milanesi non sono in grado di far fronte ad ogni sorta di pregiudizio non patrimoniale che si possa presentare all'esame dell'interprete, provocando così talvolta delle irragionevoli disparità.

[86] Cfr. Cass., SS.UU., del 11/11/2008 n. 26972.

La tutela della privacy dei minori: gli strumenti self-regulation dell'Unione Europea

FABRIZIO CORONA*

SOMMARIO: 1. Introduzione. – 2. L'online privacy risk. – 3. La tutela della privacy online dei minori in Europa come oggetto di self-regulation. – 3.1. Safer social networking principles. – 3.2. CEO coalition per far diventare internet un posto migliore per il minore. – 3.3. ICT coalition per l'uso sicuro dei dispositivi collegati e servizi online dei bambini e giovani nella UE. – 3.4. FEDMA – Federazione Europea del direct marketing. – 4. Il sistema Latzer per l'analisi degli strumenti di self-regulation. – 4.1. L'adozione degli strumenti di self-regulation. – 4.2. L'azione degli strumenti di self-regulation. – 4.2.1. Monitoraggio. – 4.2.2. Reclami e Controversie. – 4.2.3. Sanzioni. – 4.3. L'intervento del diritto sugli strumenti self-regulation. – 5. Riflessioni conclusive.

1. Introduzione.

L'area di tutela della privacy dei minori su Internet, ha recentemente assistito ad un notevole aumento di attenzione e regolamentazione da parte dell'Unione Europea. I principali fattori trainanti di questo interesse, sono la crescente importanza dei diritti del minore, compreso il diritto alla protezione dei dati personali, e le preoccupazioni relative alla loro sicurezza online. Quest'ultimo fattore è emerso come una risposta ad un forte aumento dell'utilizzo di Internet da parte di bambini sempre più piccoli. La tutela della privacy e dei dati personali in tale ambiente è diventato un requisito indispensabile per garantire la sicurezza dei minori online.

Anche se i diritti dei bambini alla privacy ed alla tutela dei dati personali sono diritti umani fondamentali e quindi la tutela della privacy dovrebbe costituire un interesse pubblico, la sua

* Avvocato, collaboratore presso la Cattedra di Logica ed Informatica Giuridica presso l'Università degli Studi di Napoli Federico II e Docente a Contratto di Informatica Giuridica presso l'Università LUISS Guido Carli.

regolamentazione, invece, è sempre passata nelle mani di attori privati. Negli ultimi anni, un insieme di soggetti legati al settore dell'ICT, si sono attivamente impegnati per concordare strumenti di autoregolamentazione (self-regulation) sul fronte della sicurezza dei bambini, tra cui la privacy e la protezione su Internet. La Commissione Europea ha svolto un ruolo significativo nel facilitare, piuttosto che dominare, questo processo normativo. Come risultato di questo processo, l'industria di Internet ha adottato diversi codici volontari di condotta, linee guida e principi. Gli sviluppi normativi concreti sono: i Principi Safer Social Network per l'Unione Europea, ossia una disposizione regolamentare tra i fornitori di servizi di social networking, il codice FEDMA, codice europeo di condotta e di autodisciplina per l'uso di dati personali nelle attività di direct marketing e le ICT e CEO coalitions dove sono stati stabiliti i principi relativi alla sicurezza ed alla privacy online dei bambini. Tali strumenti, tra gli altri obiettivi, mirano a mitigare i rischi per la privacy online, come l'uso improprio di dati personali, lo sfruttamento commerciale di tali dati ed i rischi connessi al loro utilizzo improprio. Benché il processo di autoregolamentazione e regolamentazione privata è stato presentato dalla Commissione Europea come pietra miliare nel processo di regolamentazione della tutela dei minori online, l'efficacia di tale tutela diventa fondamentale al fine di garantire una protezione effettiva. Nonostante l'evidente vantaggio che porta la soft law, come le competenze socio-tecnologiche del settore, l'innovazione, la velocità di reazione e di riduzione dei costi degli enti pubblici, è ancora percepita come una regolazione intrinsecamente debole o inefficace. Gli studiosi temono che la autoregolamentazione, come base comunitaria per la regolamentazione privata, pone problemi di legittimità, per le sue significative differenze rispetto al tradizionale modello democratico. Se la regolamentazione privata determina un'implementazione tecnica di autorità, c'è da chiedersi fino a che punto essa può avanzare un contrasto tra i vari interessi pubblici e privati[1]. Non sorprende, quindi, che per bilanciare il rapporto tra gli interessi pubblici e privati nel

[1] C. SCOTT, *Beyond Taxonomies of Private Authority in Transnational Regulation*, p. 1330.

processo di regolamentazione, l'Unione Europea abbia, col tempo, dato una maggiore attenzione al sistema di co-regolamentazione che, a causa delle diverse forme che può assumere, non garantisce sempre il suo risultato normativo.

2. L'Online Privacy Risk.

Il problema che attualmente viviamo, è che dovrebbe essere in parte mitigato da un sistema di self-regolation, riguarda la questione di come proteggere i minori. Per inquadrare tale problema, è necessario capire il significato del termine *"online privacy risk"*. Il termine on-line indica, a prima vista, una realtà virtuale dove gli utenti internet svolgono le loro attività, come ad esempio il consumo o la creazione di contenuti online. Tuttavia, per apprezzare le varie dimensioni di questo termine in relazione alle attività dei bambini online, è necessario tener presente che i bambini accedono ad internet mediante piattaforme sempre differenti e non sempre con PC desktop tradizionalmente utilizzati a casa o scuola. Sono sempre più frequenti smartphone ed altri dispositivi elettronici che sono diventati sempre più popolari in bambini sempre più piccoli.

Il rischio è un concetto complesso. Anche se generalmente inteso come *"possibilità di perdita o pregiudizio",* o *"una fonte di pericolo"*[2] non esiste una definizione universalmente riconosciuta di rischio. Le ragioni sono molteplici; in primo luogo, la comprensione di quali azioni sono a rischio ha forma diversa a seconda della cultura e della società. Come notato da Staksrud, molti fattori collettivi, come il sistema d'istruzione, i valori culturali o il quadro normativo, stabiliscono cosa possa essere percepito come pericolo dalle persone o dalle Nazioni.[3] Ad esempio, per quanto riguarda le attività dei bambini online, la loro percezione delle attività pericolose in internet, può essere dettato dall'influenza dei genitori degli insegnanti o dai stessi compagni di scuola. In secondo luogo la percezione, a livello

[2] Cfr. E. STAKSRUD, *Children in the Online World: Risk, Regulation, Rights.* London: Ashgate, 2013, p. 53.
[3] E. STAKSRUD, *Children in the Online World*, *op. cit.* p. 53.

individuale di un'attività rischiosa è spesso molto soggettiva, in quanto dipende dalla propria esperienza di vita. Quando si tratta di bambini e del loro comportamento online, i dibattiti in materia sono dominati dall'immagine del bambino come vittima impotente o utente vulnerabile. L'uso di Internet da parte dei bambini è più visto come qualcosa che può creare un rischio o pericolo, piuttosto che fornire opportunità positive. Importante notare che il rischio si riferisce alla possibilità di un pericolo, che non necessariamente avviene o si traduce in un danno. La ricerca EU kids Online ha dimostrato che non tutti i bambini che erano coinvolti in comportamenti a rischio sulla rete hanno subito un danno. Situazioni di rischio possono provocare non solo conseguenze dannose ma possono temprare il carattere e fargli acquisire maggiore resistenza e consapevolezza dei rischi sulla rete[4]. È utopico poter pensare di eliminare tutti i rischi e pericoli che la rete possa procurare ai minori che navigano, ma è opportuno garantire una responsabilizzazione degli utenti di Internet.

La privacy non è un concetto di certo meno complesso di quello di rischio. Nonostante un ampio dibattito tra filosofi, sociologi e tecnici del diritto, è ancora difficile cogliere il significato di questo concetto. L'idea di privacy come *"the right to be left alone"* coniato da Warren e Brandeis[5] implica il desiderio di agire in una zona privata, che è fuori dal controllo del pubblico.

Un approccio simile proviene da Westin, che ha definito la privacy come *"la pretesa di individui, gruppi, istituzioni di determinare per se stessi, come e in che misura le informazioni su di loro vengono comunicate agli altri"*[6]. Infine un'altra definizione è stata data da Helen Nissenbaum che definisce la privacy come *un "concetto sociale*

[4] L HASEBRINK, Uwe, Livingstone, Sonia and Haddon, Leslie (2008) *Comparing children's online opportunities and risks across Europe: cross-national comparisons for EU Kids Online.* EU Kids Online, Deliverable D3.2. EU Kids Online Network, London, UK

[5] S. WARREN, L. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, Vol. 4 (5), 1890.

[6] A.F. WESTIN, *Privacy and freedom*. 1st ed. New York: Atheneum, 1967, p.7

ed è relativo al rispetto dei limiti contestuali entro cui informazioni personali vengono condivise"[7].

Dato questo contesto, possiamo definire "online priacy risk" la possibilità di perdita di privacy nel mondo offline a causa di attività online.

3. La tutela della privacy online dei minori in Europa come oggetto di self-regulation.

Il ricorso alla self-regulation, piuttosto che alla legislazione, per tutelare la sicurezza e la privacy dei bambini online in Europa può essere fatta risalire alla metà degli anni '90. Da allora le politiche per creare un Internet più sicuro per i bambini hanno posto l'accento su strumenti normativi alternativi, come il self-regulation e la co-regulation. La preferenza per gli strumenti di self-regulation è stato confermato nella comunicazione "Strategy for a Better Internet for Children" del maggio 2012, dove si è dichiarato che *"la legislazione non verrà scartata, ma verrà data preferenza al sistema self-regulation, che resta più flessibile per conseguire risultati tangibili in questo campo"*[8]. Analogamente, l'agenda digitale per l'Europa comporta l'obiettivo di promuovere il dialogo multi – stakeholder e di self-regulation tra i fornitori di servizi europei e mondiali, come ad esempio i social network, i fornitori di comunicazioni mobili.

Attualmente, per la privacy dei minori in internet ci sono le quattro iniziative elencate nell'introduzione del presente articolo. Tre dei quattro strumenti regolamentano la sicurezza della privacy online del bambino, con principi molto simili tra loro. Il quarto strumento, il FEDMA, è utilizzato per il sistema della pubblicità online e dedica una parte alla tutela della privacy del minore nel caso di utilizzo improprio di dati personali per finalità commerciali.

---

[7] H. NISSENBAUM, *Privacy as contextual integrity*, in *Washington Law Review*, Vol.79 (119), 119-159, 2004.

[8] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Strategy for a Better Internet for Children, COM (2012) 196 Final, p. 6.

3.1. Safer Social Networking Principles.

Il Safer Social Networking Principles per l'Unione Europea è uno dei primi esempi di autoregolamentazione nel settore di sicurezza online dei minori. Avviato e sostenuto dalla Commissione Europea, questo self-regulation riunisce circa 20 servizi di social networking (SNS). Il documento delinea i sette principi dai quali i fornitori di SNS dovrebbero essere guidati che cercano di minimizzare il danno potenziale per i bambini ed i giovani e raccomanda una serie di buone pratiche e di approcci che possono contribuire al raggiungimento di tali principi.

Il primo principio si intitola *"Aumentare la consapevolezza dei messaggi di educazione alla sicurezza e le policy di utilizzo accettabile per gli utenti, genitori, insegnanti e accompagnatori in un modo chiaro ed appropriato all'età".* Con questo principio, i fornitori dovrebbero creare materiali didattici progettati per dare ai bambini ed ai giovani gli strumenti, conoscenze e competenza per navigare in modo sicuro. I messaggi devono essere presentati in un formato facile e pratico per essere compresi ed inoltre compito dei fornitori del servizio è di offrire ai genitori collegamenti mirati, materiale ed altri controlli tecnici mirati a favorire il dialogo, la fiducia ed il coinvolgimento tra genitori e figli sull'uso responsabile di Internet.

Il secondo principio, dal titolo *"Adoperarsi per garantire che i servizi siano adatti alla loro età per i destinatari"*, si stabilisce che i fornitori dovrebbero, nel normale corso di sviluppo e gestione SNS, considerare come il loro servizio può essere associato a potenziali rischi per i bambini ed i giovani. Il fornitore deve limitare l'esposizione potenzialmente pericolosa a contenuti non adatti, rendendo chiari quando i servizi non sono adatti per i bambini ed i giovani o dove è necessario l'età minima per la registrazione, adottare misure per identificare ed eliminare gli utenti minorenni dai loro servizi, adottare misure per impedire agli utenti di tentare di registrarsi nuovamente con un età diversa oppure promuovendo l'adozione del parental control.

Nel terzo principio intitolato *"consentire agli utenti attraverso strumenti e tecnologie"*, i fornitori dovrebbero utilizzare strumenti e tecnologie per aiutare i bambini ed i giovani nella gestione del

servizio, in particolare per quanto riguarda contenuti inappropriati. Le misure da adottare consentono di ridurre al minimo il rischio di contatti indesiderati o inappropriati per il minore, come ad esempio assicurando che il profilo del minore possa essere visualizzato solo dagli utenti appartenenti alla lista amici, o garantendo l'accesso alla lista amici di soli utenti con un età inferiore ai 18 anni.

Il quarto principio, dal titolo *"Fornire facili strumenti per segnalare comportamenti o contenuti che violano le condizioni di servizio",* i fornitori dovrebbero fornire un meccanismo per segnalare i contenuti inappropriati, contatti o comportamenti come indicati nelle loro condizioni generali di servizio. Tale meccanismo deve essere facilmente accessibile agli utenti in qualsiasi momento e la procedura deve essere facilmente comprensibile.

Il quinto principio si intitola *"rispondere alle notifiche di contenuto illegale o di condotta".* Al ricevimento della notifica di presunti contenuti o comportamenti illeciti, i fornitori dovrebbero avere un sistema per consentire la rimozione immediata del contenuto offensivo.

Il sesto principio, dal titolo *"Abilitare e incoraggiare gli utenti ad assumere un approccio sicuro alle informazioni personali ed alla vita privata"*, i fornitori dovrebbero fornire una gamma di opzioni di impostazione di privacy con le informazioni di supporto che incoraggi gli utenti a prendere decisioni circa le informazioni che decidono di pubblicare. Queste opzioni dovrebbero essere accessibili facilmente ed in qualsiasi momento.

Il settimo ed ultimo principio, dal titolo *"Valutare i mezzi per esaminare contenuti illegali o proibiti",* impone ai fornitori di SNS di valutare il loro servizio per identificare potenziali rischi per i bambini ed i giovani al fine di determinare adeguate procedure per la revisione e segnalazione di immagini, video e contenuti illeciti.

3.2. CEO Coalition, per far diventare internet un posto migliore per il minore.

Il CEO Coalition per far diventare internet un posto migliore per il minore, è stato progettato per raccogliere una vasta gamma di aziende private che lavorano nei vari settori della ICT (produttori di cellulari,

fornitori di sistemi, Internet service provider). Il progetto è stato lanciato dal vice presidente del Parlamento Europeo e Commissario Europeo per l'agenda digitale Neelie Kroes. In tale progetto è stato previsto di proporre e sviluppare soluzioni e misure per rendere Internet un *"luogo più sicuro per i bambini"*. Le aree in cui le società hanno deciso di agire e sviluppare soluzioni sono: strumenti semplici per gli utenti di segnalare contenuti dannosi e contatti, impostazioni privacy adeguate all'età, un uso più ampio di classificazione dei contenuti, una più ampia disponibilità e l'uso di controlli parentali, il controllo di materiale pedopornografico. A partire da gennaio 2014, 31 aziende hanno aderito al CEO Coalition. Il funzionamento della sistema si è basato su diverse forme di incontro e gruppi di lavoro: riunioni di società, riunioni di settore di attività ed incontri aperti a tutte le parti interessate.[9]

Lo stato attuale della Coalizione non è molto chiaro. Dopo il primo anno di funzionamento il progetto è stato sospeso, anche se pubblicamente i membri della Coalizione e la Commissione Europea hanno affermato il loro impegno a collaborare.

3.3. ICT Coalition, per l'uso sicuro dei dispositivi collegati a servizi online dei bambini e giovani nella UE.

Un altro simile, identico nelle sue finalità al CEO Coalition, è l'ICT Coalition. Poco prima del lancio della CEO Coalition, il settore ICT aveva realizzato una coalizione realizzando una serie di principi analoghi.

Nel primo principio, denominato *"Content"*, la coalizione ICT stabilisce che alcuni contenuti online potrebbero non essere adatti per i bambini ed i giovani. I firmatari dovrebbero pertanto: indicare chiaramente dove un servizio che offrono possa includere contenuti non considerati adatti per i bambini ed in maniera visibile opzioni che sono disponibili per il controllo dell'accesso al contenuto. Questo potrebbe includere, per il servizio, strumenti per gestire l'accesso a

[9] The CEO Coalition (2011) "Coalition to make the Internet a better place for kids: statement purpose" Retrieved 2012 07 30, from http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/ceo_coalition_statement.pdf, Annex I.f

determinati contenuti, consulenza agli utenti o di un sistema riconosciuto di contenuti. Visualizzare in una posizione facilmente accessibile la "politica d'uso accettabile", che dovrebbe essere scritta in un linguaggio facilmente comprensibile. Indicare chiaramente qualsiasi modifica ai termini di servizio o di orientamenti comunitari (vale a dire come gli utenti dovrebbero comportarsi e ciò che non è accettabile) con cui i contenuti generati dagli utenti devono uniformarsi. Assicurarsi che le opzioni di reporting siano nei settori pertinenti del servizio. Fornire avviso circa le conseguenze per gli utenti che nel postare contenuti non rispettino termini di servizio o normative comunitarie. Proseguire i lavori per fornire soluzioni innovative in grado di supportare la protezione di sicurezza per bambini con strumenti e soluzioni.

Nel secondo principio, dal titolo *"Parental Control"*, si stabilisce che i firmatari dovrebbero aiutare i genitori a limitare l'esposizione dei bambini ai contenuti potenzialmente inappropriati.

Nel terzo principio, denominato *"dealing with abuse/misuse",* si stabilisce che dove i contenuti o la condotta possa essere illegale, dannosa od offensiva, i firmatari dovrebbero fornire un processo chiaro e semplice con cui gli utenti possono segnalare contenuti o comportamenti che violino le condizioni del servizio. Implementare procedure appropriate per la segnalazione degli utenti circa immagini, video ed altri contenuti inappropriati e fornire agli utenti informazioni chiare per le eventuali procedure di revisione dei contenuti.

Nel quarto principio, *"Child abuse or illegal contact"* si stabilisce che i firmatari in caso di abuso sessuale infantile, come immagini di abusi sessuali distribuiti su internet, devono cooperare con le autorità incaricate dell'applicazione della legge, come previsto dalla legge locale e garantire la pronta rimozione di contenuti illegali contenenti le immagini con l'abuso.

Nel quinto principio *"Privacy and Control"* si stabilisce che i firmatari rispetteranno la protezione dei dati esistenti e la tutela della privacy come stabilito dalle disposizioni di legge. Inoltre, a seconda dei casi, i firmatari dovranno gestire le impostazioni di privacy appropriate per i bambini e per i giovani in modo da garantire una quanto più maggiore tutela. Offrire una gamma di opzioni di impostazione di privacy che incoraggino i genitori, bambini e giovani

a prendere le decisioni informate sul loro uso del servizio, adottare misure, se del caso e conformemente agli obblighi di legge, per informare l'utente dei diversi controlli della privacy che sono abilitati ed infine fare lo sforzo per aumentare la consapevolezza tra tutte le parti in relazione alla protezione dei bambini e dei giovani sulla rete.

Nel sesto ed ultimo principio, *"education and awareness",* i firmatari si impegnano a fornire informazioni appropriate ed impegnarsi in attività di sensibilizzazione per l'uso dei dispositivi collegati online. Lo scopo di queste attività sarà di educare i bambini ed i giovani a dare loro informazioni aggiornate per la gestione del loro accesso e le impostazioni relative ai contenuti. Fornire consigli sulle funzionalità del servizio o funzionalità che sono disponibili per consentire ai genitori la migliore protezione del minore.

Tali aree di interesse si sovrappongono con quelle della CEO Coalition. Con tali principi si obbliga una società, o gruppo di imprese, a presentare una bozza di documenti, che afferma quali obiettivi si vogliono raggiungere ed i parametri di riferimento. Le società firmatarie di questa iniziativa, sono tenute a riferire sui loro progressi in 18 mesi dopo l'adozione dei principi.

3.4. FEDMA – Federazione europea del direct marketing.

Nel 2003, la federazione europea del direct marketing ha adottato il codice europeo di condotta e di autodisciplina per l'uso di dati personali nelle attività di direct marketing. Più recentemente, nel 2010, a seguito di un ampio processo di consultazione, il codice è stato integrato con un allegato che ha aggiunto alcune disposizioni. In particolare, la Sezione 6 del codice si occupa delle "disposizioni particolari relative al Minore", dove si stabilisce che nel raccogliere dati di minori, il responsabile del trattamento dei dati dovrà sempre fare ogni ragionevole sforzo affinché il minore e/o genitore siano opportunamente informati dagli scopi del trattamento dati del minore. In particolare, nell'utilizzare materiale commerciale rivolto ai minori, o altrimenti nel raccogliere consapevolmente dati da minori, l'informativa dovrà essere posta in evidenza ed essere facilmente accessibile e comprensibile al minore.

Ove la legge nazionale o europea sulla protezione dei dati preveda il consenso dell'interessato al trattamento, il responsabile del trattamento dei dati dovrà ottenere il consenso informato e preventivo dal genitore del minore. Inoltre, il responsabile del trattamento dei dati dovrà fare ogni ragionevole sforzo per verificare che la persona che esercita il diritto del minore sia il genitore. Lo stesso responsabile non dovrà condizionare la partecipazione del minore ad un gioco, all'offerta di un premio o a qualsiasi altra attività che comporti un vantaggio promozionale al fatto che il minore divulghi più dati personali di quanti non siano strettamente necessari per partecipare all'attività.

4. Il sistema Latzer per l'analisi degli strumenti di self-regulation.

Dopo aver descritto gli strumenti self-regulation adottati all'interno dell'Unione Europea per la tutela della privacy dei minori su Internet, analizziamo se ed in che misura tali strumenti abbiano realizzato i loro obiettivi. Per conoscere bene i quattro strumenti di self-segulation, quale impatto hanno e se essi contribuiscono al raggiungimento complessivo dell'obiettivo pubblico di proteggere i minori dai rischi online, è necessario scegliere adeguati indicatori di valutazione. L'approccio più completo per valutare sistematicamente il funzionamento dei sistemi di self-regulation è stato sviluppato da Latzer nel 2007[10]. Tale approccio di valutazione tiene conto di fattori organizzativi ed istituzionali che spiegano il livello delle prestazioni alternative di regolamentazione. Questo metodo si sviluppa sull'analisi ex ante ed ex post dei sistemi di regolamentazione; nella fase ex ante si prevede la fattibilità e l'efficacia degli strumenti di self-regulation, mentre nella fase ex post si valuta la perfomance degli strumenti adottati. Il sistema valutativo si basa sul presupposto che le prestazioni di qualsiasi strumento di self-regulation è determinato da

[10] Cfr. M. LATZER, M.E. PRICE, F. SAURWEIN, S.G. VERHULST, *Comparative Analysis of International Co - and Self - regulation* in Communication Markets, Research report (commissioned by OFCOM), 2007, at: http://www.mediachange.ch/ media/pdf/publications/latzer_et_al_2007_comparative_analysis.pdf

quattro fattori: l'adozione, la consapevolezza, l'atteggiamento e l'azione. In aggiunta a tali fattori si deve considerare la particolare struttura dell'ente regolatore (fattori istituzionali/organizzativi) e dalle specifiche di mercato, ambiente ed i regolamenti (fattori contestuali). I fattori istituzionali/organizzativi sono flessibili e possono essere modificati a livello organizzativo. Essi comprendono la chiara definizione degli obiettivi, gli standard da adottare per gli strumenti di self-regulation sanzioni adeguate, periodici, revisioni esterne. Al contrario, i fattori contestuali possono essere modificati solo con la riforma di tutto il contesto normativo.

Tali fattori servono per comprendere il funzionamento di sistemi di self-regulation. Per analizzare l'impatto che tali strumenti hanno avuto nel panorama europeo, faremo riferimento ai criteri di azione e di adozione.

4.1. L'adozione degli strumenti di self-regulation.

Come notato da Bonnici, una delle principali caratteristiche degli strumenti di salf-regulation è che le regole *"siano sviluppate ed accettate da coloro che prendono parte a una attività"*[11]. Ciò significa che i soggetti privati devono tra loro riconoscere la necessità di regolamentare un determinato problema e di tradurre questa esigenza in una regola reciprocamente accettata. Nel contesto dei quattro strumenti oggetto di analisi, possiamo notare due diverse tendenze: mentre il codice FEDMA e la ICT coalition sono nati per iniziativa dei privati, la CEO coalition ed i SNS principles sono il risultato di una forte pressione della Commissione Europea. Di conseguenza, i questi ultimi due casi, manca la motivazione dei privati per affrontare i rischi della privacy online per i bambini, creando un importante fattore di diminuzione del supporto e di conseguenza la riduzione di tutto il processo di self-regulation.

Il secondo indicatore dei criteri di adozione si riferisce all'uso effettivo delle norme di self-regulation tra gli attori privati. Iniziative più efficaci sono considerate quelle in cui i partecipanti rappresentano

[11] J.P. MIFSUD BONNICI, , *Self-regulation in Cyberspace*, T.M.C. Asser Press: The Hague, 2008 p. 23.

il maggior numero possibile di potenziali attori del settore in questione. Gli SNS principles, a prima vista, appaiono come uno strumento altamente approvato dai soggetti ai quali si rivolge, raccogliendo 21 social networks providers, che rappresentano quelli più diffusi tra i giovani europei. Malgrado questo, ad un livello più ampio, i 21 social networks providers partecipanti costituiscono solo un quarto della fornitura di servizi social in Europa. Solo nel 2009-2010, l'EU Kids Online Survey ha identificato circa 80 principali social networks utilizzati nel territorio europeo; numero più che triplicato nel 2014-2015. Tenuto conto di tale stima, i SNS principles vengono scarsamente utilizzati dai titolari di social network, anche se la privacy dei loro utenti, potrebbe avere un forte impatto sulla scelta da parte dell'utente di iscriversi al servizio. Il livello di adesione è altrettanto basso nel ICT e CEO coalition, che raccolgono rispettivamente 25 e 31 aziende del settore. Anche se le coalition comprendono varie industrie e vari settori, che vanno da quelle dei cellulari, delle telecomunicazioni, social gaming, produzione di contenuti, e tenuto conto dell'elevato numero di fornitori di servizi online, il livello di rappresentazione adeguata del settore è discutibile.

In contrasto con i tre precedenti, il codice FEDMA sembra essere adottato da un organismo rappresentativo in termini di partecipazione ed appartenenza alla zona diretta di marketing online. È l'unica organizzazione in questo settore a livello dell'Unione Europea che descrive se stessa come una *"voce unica di marketing diretto e interattivo europeo*[12]*"*. L'appartenenza al FEDMA, anche se volontaria, richiede l'adozione dei suoi codici di autoregolamentazione. Il codice FEDMA rappresenta un'interessante caso di utilizzo dei membri del FEDMA. La FEDMA afferma che *"applica il codice indipendentemente da qualsiasi azienda che fa marketing diretto in Europa, anche se non si tratta di un membro di FEDMA o delle associazioni nazionali di direct marketing (DMA)."* Sembra che il suo campo di applicazione sia esteso al di là dei suoi membri e sia percepito come uno standard nel settore del marketing diretto europeo. Infine, è rilevante analizzare se i quattro strumenti godano di sostegno pubblico in termini di obiettivi e metodi di

[12] http://www.fedma.org/index.php?id=34

regolazione. Il sostegno pubblico per gli obiettivi dei quattro strumenti sopra descritti è senza dubbio elevato. Le generali preoccupazioni sui problemi di sicurezza per i bambini e la privacy online sono ben documentati da diversi rapporti e sondaggi d'opinione. Ad esempio, quasi tutti gli europei (95%) sono convinti che i minori necessitano di protezione per quanto riguarda la loro privacy e la raccolta di dati online[13]. Tuttavia esistono opinioni diverse sul metodo e modo di come tale protezione specifica dovrebbe essere garantito. Alcune iniziative, come quelle CEO coalition e SNS principles, hanno incontrato il muro della società civile e delle organizzazioni per i diritti civili a causa della loro limitata capacità di affrontare efficacemente il problema per cui sono stati realizzati. La European Digital Rights (EDRi), associazione no-profit sui diritti civili digitali, ha affermato che gli SNS principles *"hanno fatto poco più che riassumere la normativa esistente, vestendola di un approccio di autoregolamentazione"*[14], mentre la CEO coalition è stata criticata per non aver messo a fuoco il tema che si era prefissate per la debolezza degli elaborati.

Riassumendo, il codice FEDMA ha ottenuto un punteggio più alto, in quanto il numero di partecipanti al codice è più alto ed ampiamente utilizzato nel settore della commercializzazione diretta ed online. Oltre alla sua applicabilità ai membri FEDMA, il codice si applica teoricamente a qualsiasi società che faccia marketing diretto e può essere invocata dalle autorità nazionali per la protezione dei dati. Tuttavia tale strumento non ha subito un elevato coinvolgimento dalle istituzioni pubbliche. I restanti tre strumenti sono, invece, poco rappresentativi dei rispettivi settori.

4.2. L'azione degli strumenti di self-regulation.

Il criterio dell'azione si concentra sulla produzione di regolamentazione piuttosto che sul processo di regolamentazione,

[13] Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union, June 2011, in http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[14] European Digital Rights, 2013, *CEO Coalition – the blind leading the bland*, at: http://edri.org/ceo_coalition

come nel caso dell'adozione. In particolare gli strumenti di self-regulation sono valutati in termini di rispetto ed applicazione degli schemi. Altri parametri sono il numero di reclami ricevuti, le controversie trattate, le possibili sanzioni per il mancato rispetto e la presenza (o assenza) di minacce da parte delle autorità pubbliche di intervenire.

4.2.1. Monitoraggio.

Al fine di misurare il rispetto degli strumenti di self-regulation, si monitorano le diverse attività di ciascuna iniziativa. Il rispetto dei SNS principles, viene periodicamente misurata attraverso valutazioni effettuate da esperti esterni. La valutazione è stata effettuate considerando due fasi: valutazione delle singole autodichiarazioni dei SNS providers e le prove pratiche dei loro siti web. Secondo la valutazione effettuata nel 2011, solo 3 delle 14 autodichiarazioni sono state valutate come "molto soddisfacenti", mentre 9 sono state dichiarate come "piuttosto soddisfacenti" e 2 come "insoddisfacenti"[15]. Le auto-valutazioni sono state meglio valutate in base alla loro reale implementazione sui siti web ed ai problemi che gli utenti avrebbero potuto avere durante la navigazione. Per quanto riguarda la privacy, gli SNS provider hanno dimostrato la loro maggiore carenza, in quanto solo 3 su 14 sono stati dichiarati come "molto soddisfacenti". La principale debolezza dei sistemi, si è verificata in relazione alla mancanza di informazione esplicita in merito alle caratteristiche di impostazioni della privacy e la mancanza di informazioni in merito ai supporti utili per una corretta configurazione della privacy. Anche se la maggioranza degli SNS providers ha dimostrato dei progressi positivi, il settore della privacy continua a mantenere delle carenze. Analogamente agli SNS principles, la ICT coalition ha recentemente introdotto un monitoraggio indipendente per valutare come i membri della coalizione attuano i principi in materia di ICT. Diversamente dagli

[15] Assessment of the Implementation of the Safer Social Networking Principles for the EU on 14 websites: Summary Report, 2011, in http://www.unav.edu/matrimonio yfamilia/b/top/2011/UE_Donoso_Safer-social-networking-part1.pdf

SNS principles, i membri della ICT coalition sono stati valutati sulla base delle loro dichiarazioni, senza prove effettive sui loro prodotti e servizi. Tale sistema di valutazione, però, non può essere esente da critiche.

Data la tendenza dei membri a dichiarare più di quanto effettivamente attuato, solo una valutazione formale dei risultati potrebbe avere un impatto sulla valutazione obiettiva dei risultati. Il rapporto, sembra più una sintesi di buoni risultati, piuttosto che una valutazione obiettiva.

Il CEO coalition non subisce alcun sistema di monitoraggio formale. Il monitoraggio è stato effettuato durante il primo anno di funzionamento del CEO, ma era stato molto vago. Nel complesso si era riconosciuto che il progresso era stato effettuato in tutte e cinque le aree di lavoro. Nel Febbraio 2013, l'amministratore delegato della CEO coalition ha pubblicato la sua relazione finale contenente raccomandazioni e migliorie da poter adottare, mentre nel gennaio 2014, le imprese individuali hanno prodotto relazioni distinte su come hanno adottato ed adotteranno le raccomandazioni della coalizione. La situazione, almeno sulla carta, è differente per il codice FEDMA che adotta un meccanismo di monitoraggi specifico. L'onere del monitoraggio è affidato ad un "Comitato per la protezione dei dati" che è stato istituito per monitorare l'applicazione del codice.

4.2.2. Reclami e Controversie.

Teoricamente l'applicazione dipende dall'esistenza e dalla possibilità di accedere alle procedure per gestire possibili reclami in relazione alle norme di self-regulation e le conseguenze per i membri in caso di violazione. L'unico strumento self-regulation che prevede una procedura di ricorso è il codice FEDMA. Tale codice, essendo uno strumento europeo, dedica una parte alla definizione delle procedure per risolvere eventuali reclami che possono derivare dall'applicazione del codice stesso. Il reclamo viene analizzato dal "Comitato per la protezione dei dati", organo interno, composto da rappresentanti di associazioni nazionali di marketing diretto, il FEDMA e le aziende che sono membri diretti del FEDMA.

4.2.3. Sanzioni.

Altra carenza che si verifica nella maggior parte degli strumenti di self-regulation, è la mancata esecuzione delle sanzioni quando le violazioni delle norme di autoregolamentazione si verificano. Tale carenza si verifica per l'assenza di organismi specifici in grado di far rispettare tale sanzione. Un riferimento esplicito alle sanzioni è presente solo nel codice FEDMA. Ai sensi del codice, le associazioni nazionali di direct marketing sono responsabili per l'applicazione del codice e devono applicare le stesse sanzioni previste nei loro paesi per il mancato rispetto dei loro codici nazionali. Inoltre, a seconda del tipo di violazione, il Comitato per la protezione dei dati può raccomandare al FEDMA di espellere un membro o applicare sanzioni[16]. Nella pratica non è chiaro quante volte la FEDMA abbia applicato come sanzione l'espulsione. Inoltre FEDMA non è in grado di imporre multe o applicare sanzioni monetarie, poiché è un'organizzazione di adesione volontaria.

In misura minore, ma simile, una possibilità sanzionatoria è presente nell'ICT Coalition. Si afferma che "se un membro non intende applicare i principi, può essere sottoposto ad esclusione". Tuttavia, non è ancora possibile sapere in che misura la ICT coalition abbia applicato tale principio. Altre due iniziative vengono utilizzate come meccanismi sanzionatori simbolici, connessi alla "reputazione delle imprese". Nel caso di scarso rendimento o non conformità ai SNS Principles, la Commissione Europea non ha mezzi formali per migliorare il rendimento, ma può pubblicare "rimproveri" verso le aziende che non riescono a rispettare tali principi. Tale sanzione simbolica può essere applicata nel caso del CEO coalition.

4.3. L'intervento del diritto sugli strumenti self-regulation.

L'intervento del diritto da parte delle autorità pubbliche è considerato come un ulteriore incentivo da adottare per far rispettare le norme self-regulation. Oltre all'intervento esplicito, l'importanza e l'interpretazione del diritto vigente nell' Unione Europea, non

[16] Codice FEDMA p.18

dovrebbe essere scartato. Anche se le istituzioni comunitarie non hanno mai minacciato pubblicamente le imprese con precise disposizioni di legge qualora gli strumenti self-regulation non fornissero i risultati attesi, alcuni segni indicano che la Commissione Europea si stia muovendo in tale direzione. Nel contesto della revisione del quadro di protezione dei dati personali, una possibilità di affrontare la protezione della privacy del minore è stata considerata. La consultazione pubblica, ha rivelato la volontà delle aziende di sviluppare dei codici di condotta in combinato disposto con l'art. 29 Working Party, per garantire la concreta applicazione. Appare discutibile, però, che l'intervento della Commissione Europea attraverso la protezione dei dati, abbia avuto influenza su una migliore osservanza dei regimi di self-regulation.

Un punteggio basso sulla conformità al diritto, può esser assegnato alla CEO coalition, dove si valuta il loro lavoro, senza una supervisione o controllo esterno. In questo modo non è possibile stabilire quanto le singole imprese seguano i consigli e le migliori pratiche previste dalla coalizione. Un livello di conformità più chiaro, seppure basso, è dato nel SNS Principles, dove vengono effettuate valutazioni indipendenti. Tuttavia in caso di scarsa aderenza, non vi è possibilità di applicare sanzioni efficaci e commercialmente significative. La ICT coalition, ha una indipendente procedura di monitoraggio e prevede la possibilità di escludere aziende che che violino i principi in materia di ICT. Il codice FEDMA ha tutti gli aspetti necessari a garantire e misurare la conformità: una struttura organizzativa, una procedura di reclamo e potere sanzionatorio. Tuttavia, questo non garantisce le periodiche revisioni e valutazioni.

Pertanto, anche se promettente sulla carta, il codice FEDMA nella pratica non assume tale efficacia.

5. Riflessioni Conclusive.

Il raggiungimento del self-regulation in un settore delicato come quello della privacy del minore, non è facile malgrado siano stati realizzati quattro strumenti per raggiungere tale finalità. Sulla base dell'analisi effettuata utilizzando il sistema di Latzer, si è visto come i

quattro strumenti, il safer social networking, il CEO coalition, l'ICT coalition ed il FEDMA non abbiano ottenuto i risultati sperati. Una possibile risposta alle attuali carenze, potrebbe rinvenirsi nell'intervento da parte della Commissione Europea ad un approccio di co-regolamentazione più forte e meglio definito sul fronte della sicurezza online del minore. Tale soluzione potrebbe essere attuata, in quanto l'area della privacy dei bambini su Internet difficilmente può essere immaginata come solo strumento di self-regulation. Realizzare degli strumenti self-regulation che, magari, hanno una buona struttura normativa, ma non sorretti da una forte e decisa politica di sanzioni sottoposta ad un controllo da parte dell'Unione Europea, porta facilmente gli operatori del diritto a non rispettare tali strumenti. Solo un buon strumento di co-regolamentazione è in grado di realizzare innovazione, consentire un apprendimento reciproco, sensibilizzazione, condivisione di risorse tra gli operatori e le altre parti interessate.

Ciò risulta in linea con il ragionamento della Commissione Europea, dietro la creazione di piattaforme multi-stakeholder normative. Come spiegato da Neelie Kroes *"Abbiamo bisogno di incoraggiare l'innovazione, scambiare idee e condividere le risorse. E abbiamo bisogno di continuare a costruire un'infrastruttura trans-europea per tutelare e proteggere i bambini(...)"*[17].

[17] N. KROES Vice-President of the European Commission responsible for the Digital Agenda Making Internet a better place for children – a shared responsibility Safer Internet Forum 20 October 2011, Luxembourg, Reference: SPEECH/11/703, 20/10/2011, at http://europa.eu/rapid/press-release_SPEECH-11-703_en.htm

Criticità dell'applicazione dei principi di safe harbour nella tutela dei dati personali di cittadini europei

LUIGI PRINZI*

SOMMARIO: 1. Background: richiamo sui principi di Safe Harbour. – 2. Background: strumenti alternativi di trasferimento fuori dall'Unione europea di flussi di dati. – 3. Background: Giudizi di merito sull'efficacia del Safe Harbour ed evoluzione dell'accordo Safe Harbour – 4. La sentenza della Corte di Giustizia europea – 5. Valutazioni in ambito comunitario della sentenza della Corte di Giustizia europea e suoi effetti. – 6. Prime ripercussioni della sentenza nel mondo della privacy. – 7. Valutazioni finali.

1. Background: Richiamo dei principi Safe harbour

Il quadro normativo-regolamentare applicato negli USA in fatto di protezione dei dati personali non è stato riconosciuto dalla Commissione della UE come uno che assicuri una protezione 'adeguata', in quanto negli USA non sussiste una legge generale di tutela dei dati. Ciò deriva dal fatto che il suddetto quadro è tradizionalmente fondato su una combinazione di norme specifiche della privacy e di codici di autoregolamentazione, piuttosto che una regolamentazione unitaria e generale in materia di dati personali secondo le linee della Direttiva 95/46/CE di tutela dei dati personali o le leggi del suo recepimento nei vari Stati dell'Unione. Nonostante vantino una solida tradizione culturale in fatto di diritto alla privacy e quindi di *informational privacy*, gli USA hanno preferito interventi settoriali federali, cui si sono talora affiancati interventi specifici di fonte statuale[1]. Inoltre nel campo soprattutto del commercio, la tutela dei dati, affidata prevalentemente all'autoregolamentazione, si è dimostrata carente, sia per quanto riguarda l'informativa al

* Consulente per il settore delle reti e dei servizi di comunicazioni elettroniche.

[1] Cfr. A. MANTELERO, *Data Protection ed attività d'impresa. Verso dove guardano gli USA?* in *Dir. Inf. Inf.*, n. 3, 2011.

consumatore, spesso incomprensibile per lui, circa le policies adottate dal fornitore in materia di privacy, sia con riferimento al diritto d'accesso, come ammette la stessa Federal Trade Commission (FTC) fautrice del principio *notice and choice model* basato sostanzialmente sul consenso implicito (regime dell'*opt-out*[2]), con riflessi inevitabilmente negativi sulla sicurezza dei dati[3].

Al fine di colmare questo gap tra regolamentazione della privacy nel campo dei dati personali in USA e nell'Unione, particolarmente evidente alla fine degli anni Novanta, il Dipartimento del Commercio degli USA e la Commissione europea hanno sviluppato l'Accordo quadro U.S.-EU Safe Harbour (Approdo sicuro), tuttora vigente, in materia di tutela dei dati negli scambi commerciali tra mercato comunitario ed imprese statunitensi. Più precisamente il suddetto Accordo è sancito dalla Decisione della Commissione europea del 26 luglio 2000[4] (*Safe Harbour Decision*), presa ai sensi dell'art. 25(6) della 95/46/C[5], che stabilisce l'adeguatezza alla normativa comunitaria (direttiva 95/46/CE) del trattamento dei dati personali di cittadini europei trasferiti negli USA da parte di organizzazioni statunitensi che aderiscono al suddetto Accordo. Pertanto la suddetta Decisione fornisce una base legale per il trasferimento di dati personali dall'Unione Europea a compagnie stabilite negli USA che siano dotate della certificazione Safe Harbour, ossia che si siano

[2] Il regime *opt-out* si fonda sulla presunzione del consenso dell'interessato, fatta salva la condizione in cui lo stesso può indicare il proprio diniego per alcune o tutte le operazioni di trattamento dei dati che lo riguardano. Il meccanismo *opt-in*, invece, implica che il trattamento dei dati personali possa essere avviato solo con il consenso esplicito, libero e informato dell'interessato.

[3] *ibidem*

[4] COMMISSIONE EUROPEA, Decisione 2000/520/CE, *a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti*, in *GUCE*, L 215 del 25 agosto 2000, p. 7.

[5] L'articolo 25 e l'articolo 26 della direttiva sulla protezione dei dati stabiliscono il quadro giuridico per il trasferimento dei dati personali dall'UE a paesi terzi al di fuori del SEE rispettivamente in Paesi in cui la tutela dei dati è adeguata/non adeguata alle norme della direttiva in considerazione della sua legislazione nazionale o degli impegni internazionali.

impegnate formalmente all'osservanza dei principi di privacy in essa contemplati[6]. L'accordo "Safe Harbour" è, quindi, una politica di compromesso per il superamento delle difficoltà incontrate dalle compagnie USA che operano sul mercato comunitario ad attenersi alle norme di protezione dei dati personali dei cittadini europei verso i quali sono fornitori di beni/servizi, fissate dalla direttiva di cui sopra, dal momento che esse risultano più stringenti della normativa e delle procedure attualmente in vigore negli USA[7].

Il suddetto accordo richiede che le compagnie statunitensi che sono abilitate a sottoscriverlo[8] secondo quanto prevede la legislazione Americana e che desiderano aderirvi, si impegnino, sottoscrivendo una procedura di autocertificazione, al rispetto di 7 principi in materia di trattamento dei dati personali, da applicare in conformità agli orientamenti forniti da talune FAQ, che fanno parte integrante della succitata Decisione. Questi principi, figuranti nell'allegato I della decisione Approdo sicuro, impongono alle compagnie:

- di informare gli interessati circa le finalità della raccolta di dati atti ad identificarli, le modalità di contatto per la ricezione di eventuali quesiti o reclami espressi dagli stessi e chi siano i terzi ai quali vengono rivelati questi dati informativi (I principio, di notifica);
- di consentire agli interessati di esprimere il rifiuto (modalità di scelta *opt out*) che i loro dati – non sensibili – siano trasmessi a terzi o siano

[6] Nel nostro paese, il Garante della privacy, preso atto della suddetta decisione comunitaria, il 10 ottobre 2001 ha concesso l'autorizzazione alle organizzazioni aventi sede negli USA ed aderenti all'accordo "Safe Harbour", a trasferire i dati personali dall'Italia verso gli USA.

[7] Gli USA adottano un approccio settoriale basato su di un mix di norme giuridiche, regolamentazione ed autoregolamentazione. L'Unione Europea, invece, si basa su di una legislazione esauriente, che richiede, tra l'altro, la creazione di Autorità di tutela dei dati indipendenti, registrazione dei database presso dette Autorità e in alcuni casi una loro preventiva autorizzazione prima che il trattamento dei dati possa aver luogo.

[8] Solo le organizzazioni statunitensi soggette alla giurisdizione del Federal Trade Commission (FTC) o quelle soggette alla giurisdizione del Department of Transportation (DoT), tra cui compagnie aeree statunitensi, possono partecipare al programma Safe Harbour. Le organizzazioni generalmente non soggette alla giurisdizione FTC includono alcune istituzioni finanziarie (ad esempio banche), gestori di TLC, associazioni , organizzazioni no-profit.

usati in modo incompatibile con lo scopo per il quale furono raccolti o con quello successivamente autorizzato (II principio, di scelta);
- di chiedere il consenso degli interessati circa la trasmissione dei dati ad un terzo nell'osservanza dei primi due principi (III principio, di trasferimento successivo);
- di garantire la *security*, ossia la protezione da rischi di perdita, abuso, uso non autorizzato, distruzione dei dati (IV principio, di sicurezza);
- di garantire l'integrità dei dati, ossia l'affidabilità in relazione all'uso previsto e l'accuratezza (V principio, di integrità dei dati);
- di consentire agli interessati di accedere ai dati raccolti, di richiederne la modifica se inaccurati o la cancellazione (VI principio, di accesso);
- infine di predisporre i mezzi atti a garantire l'osservanza dei principi Safe Harbour e la possibilità di ricorso degli interessati i cui legittimi interessi siano stati lesi da una loro violazione (VII principio, delle garanzie di applicazione, ossia "*Enforcement Principle*").

In sintesi i suelencati principi sono rivolti sia alla protezione materiale dei dati personali (principi riguardanti l'integrità dei dati, la sicurezza, la scelta e i trasferimenti successivi), sia la garanzia dei diritti procedurali degli interessati (principi riguardanti la notifica, l'accesso e le garanzie d'applicazione).

L'impresa che aderisce all'accordo Safe Harbour deve inviare annualmente una autocertificazione al Dipartimento del Commercio USA in cui dichiara di ottemperare alle clausole previste da questo Accordo traducentisi nei principi suesposti. Inoltre deve anche specificare nel suo statement della policy della privacy, riportato sul proprio sito web, che aderisce all'Accordo in parola. Ad esempio, sul proprio sito, la Microsoft, in veste di cloud provider, riporta le condizioni della privacy alle quali si attiene, ossia il *privacy term windows azure* nei termini "*salvo ove diversamente specificato all'interno di un Servizio, le informazioni raccolte da o inviate a Microsoft potranno essere archiviate ed elaborate negli Stati Uniti o in qualsiasi altro Paese in cui siano presenti Microsoft, le sue consociate, le sue filiali o i provider di servizi. Microsoft rispetta la convenzione Safe Harbour stabilita dal Ministero del Commercio degli Stati Uniti relativamente alla raccolta, al trattamento e alla*

detenzione di dati di utenti dei Paesi dell'Unione europea, dell'Area Economica Europea e in Svizzera".

Le organizzazioni devono inoltre rendere note pubblicamente le loro politiche in materia di riservatezza e sono sottoposte all'autorità della Commissione federale per il commercio (FTC) ai sensi della sezione 5 del Federal Trade Commission Act, che vieta attività o pratiche sleali o ingannevoli in materia commerciale o collegata al commercio, oppure di altri organismi istituiti con legge in grado di assicurare efficacemente il rispetto dei principi applicati in conformità alle FAQ.

Affinché le organizzazioni che aderiscono ai principi ed alle FAQ possano essere riconosciute dalle parti interessate, quali le persone che sono oggetto dei dati, gli esportatori di dati e le autorità per la protezione dei dati, il Dipartimento del commercio degli Stati Uniti, o l'ente da esso designato, deve assumersi il compito di compilare e rendere disponibile al pubblico un elenco delle organizzazioni che autocertificano la loro adesione ai principi applicati in conformità alle FAQ e sono sottoposte all'autorità di almeno uno degli enti governativi di cui all'allegato VII della presente decisione. Considerato quanto sopra detto, si può confermare la convergenza dei principi "Safe Harbour" alle disposizioni normative EU in materia di Privacy, pur dovendo riconoscere che il livello di garanzia della protezione dei dati da essi offerto è necessariamente minore di quello derivante dall'osservanza della direttiva comunitaria. Ciò in quanto detti principi sono frutto di una negoziazione – rispecchiata nella decisione della Commissione europea del 2000 – in cui il peso della controparte statunitense è stato evidentemente rilevante.

Sul piano della prassi operativa del Safe Harbour, invece, le stesse Autorità di controllo europee nutrono da sempre non pochi dubbi circa un'effettiva adeguatezza alla normativa comunitaria della certificazione sottoscritta dalle imprese stabilite negli USA dell'osservanza delle norme di privacy contemplate dall'Accordo. Si segnala a tale riguardo che il Garante tedesco della privacy ha stabilito con una delibera del 29 aprile 2010 che – non sussistendo a suo giudizio verifiche ad ampio raggio da parte delle autorità di controllo sull'una e l'altra sponda transatlantica – la certificazione Safe Harbour non sarebbe di per sé idonea ad offrire adeguate garanzie di protezione

dei dati nel contesto dei servizi Cloud che prevedono due parti contrattuali, una in veste di esportatore di dati tra cui quelli personali, di norma nel ruolo di "controller" (responsabile del trattamento dei dati) e l'altra in veste di "processor" e di importatore di dati, ed una terza parte beneficiaria, rappresentata dall'interessato (*data subject*). La stessa autorità ha raccomandato, pertanto, all'impresa esportatrice operante in Germania di controllare attivamente che l'impresa importatrice dei dati metta correttamente in pratica i principi di Approdo sicuro per quanto riguarda la riservatezza ed anche in materia di doveri di informazione nei confronti dell'interessato i cui dati personali sono oggetto di trattamento, e verifichi almeno che la certificazione Approdo sicuro dell'importatore sia sempre valida.

Il 24 luglio 2013, a seguito delle rivelazioni di Snowden sui programmi di controllo disposti dalla NSA statunitense, il Garante tedesco ha affermato come "*sia molto probabile che i principi enunciati nelle decisioni della Commissione vengano violati*". Per contro il Garante irlandese in relazione a due denunce riguardanti il regime Approdo sicuro, giunte dopo le notizie sull'attività della NSA, si è rifiutata di svolgere indagini, sostenendo che il trasferimento di dati personali verso il paese terzo non violava le condizioni della legislazione irlandese.

Quanto sopra dimostra che le reazioni alle rivelazioni sui programmi americani di controllo da parte delle autorità per la protezione dei dati europee sono state divergenti.

2. Background: Strumenti alternativi di trasferimento fuori dall'Unione europea di flussi di dati

I principi "Safe Harbour" costituiscono un quadro normativo di tutela dei diritti fondamentali della privacy negli USA adeguato alle norme comunitarie, secondo quanto stabilito dalla Decisione della Commissione n. 2000/520/CE. Peraltro, sussistono e trovano largo impiego strumenti normativi alternativi al suddetto quadro, in particolare le *Standard Contractual Clauses* (SCC) e le *Binding Corporate Rules* (BCR) previste dall'articolo 26 della Direttiva 95/46/CE, autorizzate dalla Commissione (SCC) o dalle autorità

garanti della privacy (BCR) per fini di trasferimento di specifici flussi di dati in Paesi, il cui regime di tutela dei dati non è giudicato adeguato da parte della Commissione. Le SCC inserite nel contratto stipulato tra l'importatore e l'esportatore dei dati in un paese esterno all'Unione garantiscono il trattamento dei dati conformemente ai principi stabiliti dal diritto comunitario anche in questo paese. Le BCR costituiscono un singolo *set* di regole vincolanti per tutte le entità di una società multinazionale nel trasferimento dei dati tra esse e loro successivo trattamento, e quindi disciplinano particolari flussi di dati trasferiti esternamente al territorio dell'Unione, assicurando nel contempo lo stesso elevato livello di protezione dei dati personali all'interno del gruppo.

Ai sensi dell'articolo 26(2) of Directive 95/46/EC, i predetti strumenti introducono appropriate salvaguardie dei fondamentali diritti alla privacy e del loro esercizio da parte del *data subject*, della cui osservanza viene investito il *controller*, ossia la parte che stabilisce le finalità ed i mezzi per il trattamento dei dati. La Commissione ha approvato, in accordo con l'articolo 26(4) della Direttiva 95/46/CE, quattro pacchetti di clausole modello SCC che soddisfano i requisiti dell'articolo 26(2) della Direttiva; due pacchetti di *model clauses* si riferiscono a trasferimenti tra controller, mentre gli altri due a trasferimenti tra un controller ed un processor che, per definizione di tale ruolo, ne esegue le istruzioni. Le suddette clausole fissano i rispettivi obblighi in capo all'esportatore ed all'importatore dei dati, relativamente a compiti quali l'attuazione di:

- misure di sicurezza;
- notifiche all'esportatore dei dati di richieste d'accesso ad essi espresse da autorità giudiziarie di un paese terzo o di un avvenuto accesso accidentale o non autorizzato;
- diritti del soggetto dei dati all'accesso, alla loro rettifica e cancellazione;
- misure di compensazione a suo favore nel caso di danno da lui subito per violazione delle SCC da una delle parti.

Esse inoltre attribuiscono al soggetto dei dati dell'Unione europea la facoltà di presentare istanza presso l'Autorità di protezione dei dati o la Corte di Giustizia dello Stato membro in cui l'esportatore dati è stabilito, mirante a far valere i diritti che le clausole contrattuali gli

riconoscono quale parte beneficiaria. L'iscrizione dei suelencati obblighi e dei diritti del soggetto dei dati nelle clausole contrattuali SCC ha la sua ragion d'essere nell'essere in esse previsto il trasferimento dei dati in un paese terzo nel quale, non essendovi applicate norme statali di privacy adeguate a giudizio della Commissione, è da presumere che l'importatore dei dati non sia oggetto di un sistema di controllo efficace dell'attuazione delle norme sulla privacy e d'imposizione della loro osservanza in caso di inadempienza. In assenza di una decisione di adeguatezza in base all'articolo 25(6) della Direttiva 95/46/EC, come ad esempio nel caso del Safe Harbour, ed indipendentemente dall'impiego delle SCC e/o BCR, i dati personali possono ancora essere trasferiti in un paese terzo a condizione, però, che il soggetto dei dati abbia espresso il suo consenso, una volta che sia stato informato sui rischi del trasferimento, in maniera inequivocabile; il trasferimento in un paese extra-UE può avvenire anche nei seguenti casi di derogazione dalle norme sulla privacy in tema di trasferimenti ai sensi dell'articolo 26(1):

- perfezionamento di accordi commerciali stipulati dal soggetto dei dati ed il controller (es. prenotazione alberghiera, o quando un'informazione di pagamento è trasferita in una banca di un paese terzo);
- implementazione di misure precontrattuali su richiesta del soggetto dei dati;
- tutela di interessi vitali del data subject;
- motivazioni importanti di pubblico interesse;
- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

3. Background. Giudizi di merito sull'efficacia del Safe Harbour ed evoluzione dell'accordo

Fin dall'emanazione della Decisione della Commissione 2000/520/CE si dava per acquisito che questa sorta di autocertificazione delle aziende americane fosse sufficiente, sul piano giuridico, a garantire il diritto alla privacy dei cittadini europei, ma valutazioni critiche negative sono state espresse, nel corso degli anni,

a più riprese da varie Autorità di protezione dei dati od organi di consultazione circa un'efficace tutela dei dati trasferiti negli USA in applicazione del Safe Harbour. Peraltro, con riferimento in particolare all'Accordo Safe Harbour occorre tener presente che il Dipartimento del Commercio degli USA e la Commissione dell'UE hanno pubblicamente riaffermato in un documento a firma congiunta del marzo 2012[9] il loro impegno a mantenere in vigore l'accordo di cui sopra, in linea con gli obiettivi di accrescere gli scambi commerciali tra UE e USA e l'interoperabilità dei rispettivi regimi normativi della privacy nell'uso dei dati personali per finalità commerciali ed il rafforzamento della cooperazione nell'adozione delle misure esecutive. Ciò alla luce anche di un profondo processo di ridefinizione della privacy pure negli USA a seguito dell'emanazione il 23 febbraio 2012 da parte del Presidente Obama del blueprint sulla tutela dei dati, in cui figura il *Consumer Privacy Bill of Rights*, che è passato all'iter legislativo per l'eventuale approvazione da parte del Congresso ai fini della sua adozione nei settori commerciali, non soggetti alle vigenti leggi federali sulla privacy, attraverso lo sviluppo di codici di condotta di implementazione dei principi in esso contenuti, al termine di un processo che vedrà la partecipazione di una molteplice tipologia di stakeholder (portatori di interesse), compresi i consumatori. Nel corso del meeting del 10 ottobre 2013 del Comitato interparlamentare europeo in merito alla riforma del quadro della protezione dei dati, la stessa vice-presidente della Commissione Europea Viviane Reding ha affermato che detta riforma non inciderà sul Safe Harbour, che pertanto sarà mantenuto in vigore. La Comunicazione della Commissione del 27 novembre 2013[10] ha ribadito l'importanza del mantenimento[11] dell'Accordo Safe Harbour, divenuto, a partire dalla

[9] U.S.-EU *Joint Statement on Privacy from EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson*, March 19, 2012.

[10] EUROPEAN COMMISSION, COM(2013) 847 final, *Communication from the Commission to the European Commission and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, 27.11.2013.

[11] Secondo la COM(2013) 847 final, se i servizi e i flussi di dati transfrontalieri dovessero subire perturbazioni a seguito delle soppressione di norme vincolanti d'impresa, di clausole contrattuali tipo e del regime di Approdo sicuro, l'impatto

sua adozione nel 2000, un veicolo insostituibile per i flussi di dati UE-US, che hanno manifestato una crescita esponenziale – unitamente al numero di imprese importatrici negli USA – se soltanto si pensa alle centinaia di milioni di clienti in Europa di compagnie web quali Google, Facebook, Microsoft, Apple, Yahoo. Secondo la summenzionata Comunicazione, al 26 settembre 2013 il numero di organizzazioni certificate indicate nell'elenco Approdo sicuro come "Attuali" era 3246, tra imprese sia di piccole che di grosse dimensioni.

Il documento di cui sopra, facendo seguito alle due relazioni di valutazione del funzionamento del Safe Harbour del 2002 e 2008, con riferimento agli interessi dei cittadini europei e delle imprese stabilite nell'Unione, riconosce le funzioni positive che detto Accordo ha svolto in tutto questo tempo nello sviluppo dell'economia digitale, pur non mancando di sottolinearne, con puntuale e rigorosa disamina, non pochi malfunzionamenti intervenuti nel decennio dalla sua validità, cui solo assai limitatamente la FTC (Federal Trade Commission) statunitense, ossia il Dipartimento del commercio ha posto rimedio. Una delle azioni della FTC è stata quella di obbligare le imprese Approdo sicuro di presentare sul loro sito web pubblico la loro politica in materia di riservatezza dei dati degli interessati e di inserire il link al sito web Approdo sicuro del Dipartimento, in cui è memorizzato l'elenco delle imprese certificate Safe Harbour. Le inadempienze riguardano la sostanziale mancanza di trasparenza talora delle imprese partecipanti al Safe Harbour, l'applicazione effettiva dei Principi della privacy previsti dall'Accordo da parte delle compagnie statunitensi aderenti, la necessità di una maggiore efficacia delle misure attuate finora dalle autorità negli USA o di altre ancora per il rispetto dell'osservanza, non poche volte elusa, delle correlative norme di condotta da parte delle medesime. La FTC si sforza di individuare, attraverso anche proprie valutazioni indipendenti, violazioni degli impegni di Approdo sicuro, tra cui presentazioni ingannevole da parte dell'impresa della propria prassi in materia di

negativo sul PIL dell'UE potrebbe essere compreso fra -0,8% e -1,3%, e le esportazioni di servizi dall'UE agli USA calerebbero al -6,7% a causa della perdita di competitività. Si veda: "*The Economic Importance of Getting Data Protection Right*", studio del Centro europeo per la politica economica internazionale per la Camera di Commercio statunitense, marzo 2013.

privacy, e delle azioni avviate, non molte per la verità, alcune si sono tradotte nell'irrogazione di pene pecuniarie, come ad esempio quella di 22,5 M.ni inflitta dalla FTC a Google.

I suddetti rilievi della Commissione si traducono (nella predetta Comunicazione del 27 novembre 2013) in una serie di tredici raccomandazioni rivolte alle Autorità statunitensi responsabili dell'applicazione del Safe Harbour Framework, che erano state invitate a trovare gli opportuni rimedi entro l'estate 2014. Esse richiedono innanzitutto che la FTC esplichi controlli più estesi sull'applicazione di misure più efficaci che le imprese certificate dovrebbero adottare in tema di trasparenza, tra cui, oltre a quelle più sopra discusse, le condizioni di tutela della privacy figuranti in ogni contratto concluso con appaltatori, ad esempio con servizi di cloud computing. L'Approdo sicuro consente trasferimenti successivi dalle imprese aderenti a terzi che agiscono in qualità di rappresentanti, ad esempio fornitori di cloud, ma secondo la Commissione essi dovrebbero essere disciplinati da un contratto stipulato tra l'impresa certificata ed il Cloud provider e le garanzie sottoscritte relativamente alla privacy dovrebbero essere rese pubbliche. Inoltre, viene anche raccomandato dalla Commissione che sul sito web dell'impresa certificata compaia un link che rinvii al prestatore incaricato della risoluzione alternativa delle controversie (ADR) e/o al Comitato UE per la tutela dei dati e viene anche richiesto che l'ADR sia di pronto impiego e di costo abbordabile per l'interessato e sia controllato più sistematicamente dal Dipartimento del Commercio per quanto attiene, ad esempio, alla trasparenza della modalità di offerta dei servizi, in modo che la procedura ADR sia un meccanismo efficace, fidato e di successo. É assolutamente necessario poi, secondo la Commissione, che le imprese auto-certificate precisino nella loro policy in che misura la legislazione americana consente alle pubbliche autorità di raccogliere e trattare i dati trasferiti nel quadro del regime Approdo sicuro ed esplicitino i casi in cui le imprese, dovendosi adeguare ad essa, applicano eccezioni, peraltro in misura strettamente necessaria e proporzionata, ai principi per esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia.

Nel discorso del 9 dicembre 2013 "*Mass surveillance is unacceptable- US action to restore trust is needed now"*, il

vicepresidente dell'Unione europea Viviane Reding, dopo aver stigmatizzato il comportamento della National Security Agency, ricollegandosi alle suddette raccomandazioni, aveva espresso la necessità che l'Accordo Safe Harbour sia reso più sicuro e che il suo funzionamento venga rivisto successivamente al loro accoglimento. Ha formulato inoltre il forte auspicio che venga accolta la raccomandazione sul reindirizzamento (*redress*) giudiziario, di cui dovrebbero beneficiare i cittadini europei non residenti negli USA, basato su un link che le imprese americane aderenti al Safe Harbour dovrebbero inserire nella loro policy sulla privacy online di collegamento a un provider alternativo competente nella risoluzione di dispute ("Alternative Dispute Resolution", ADR), tra cui l'EU Data Protection Panel, il provider europeo che svolge il medesimo ruolo, che l'interessato (il "data subject") possa contattare direttamente e trovare prontamente disponibile a trattare il suo reclamo ed a prezzi sostenibili. Si tratta del resto di un diritto dell'interessato il cui riconoscimento è sancito dal principio di "enforcement" del Safe Harbour che prescrive il suo diritto all'accesso ad un meccanismo indipendente di risoluzione della disputa "*readily available and affordable*". In realtà non si può dire che il principio venga osservato nella sua interezza, se è vero che correntemente i prezzi dei provider ADR statunitensi nell'ambito dello schema Safe Harbour per la gestione di reclami sono di circa 200-250 $, mentre in Europa il servizio di risoluzione dello stesso reclamo, rivolgendosi la persona all'European Data Protection Panel, è gratuito[12].

4. La sentenza della Corte di Giustizia europea

Con la sua sentenza del 6 ottobre 2015 (causa C-362/14 Schrems/Data Protection Commissioner) la Corte di Giustizia Europea, pur pronunciandosi sul singolo ma emblematico caso trattato e risolto col dare indirettamente ragione al ricorrente Schrems[13], che

[12] *ibidem*

[13] La denuncia presentata dallo studente di giurisprudenza austriaco Schrems all'autorità irlandese per la protezione dei dati (essendo in Irlanda la sede della filiale

sosteneva l'illegittimità del trasferimento dei suoi dati da parte di Facebook negli USA, chiedendone pertanto la cancellazione in quanto esso sarebbe rispondente ad un approccio generalizzato seguito dalle Autorità statunitensi[14] lesivo della privacy, ha dichiaratamente destituito di validità la Decisione della Commissione del 26 luglio 2000, relativamente al trasferimento dei dati in USA. A tale riguardo, la Corte fa rilevare che il regime del Safe Harbour, mentre è vincolante per le imprese americane che lo sottoscrivono, non impegna in alcun modo le autorità pubbliche degli Stati Uniti. Ma, cosa ancor più rilevante, è la prevalenza, sottolineata nella sentenza, della sicurezza nazionale, del pubblico interesse e delle leggi statunitensi, senza che sia attuato un compromesso tra interessi contrastanti, sui principi del "Safe Harbour", che le imprese sono nella prassi autorizzate a violare ogni volta che configgano con dette esigenze, lasciando libera la via all'accesso generalizzato ai dati alle autorità pubbliche statunitensi finalizzato esclusivamente al loro controllo e talora in maniera sproporzionata alla tutela della salvaguardia della nazione. La Corte ha dichiarato quindi che principi normativi – sulla cui applicazione, peraltro non viene effettuato alcun controllo da parte di un'Autorità di garanzia – che consentono un'ingerenza pubblica nella sfera personale, "*deve essere considerata*

europea del social network americano), sottolineava l'inadeguatezza del diritto e delle prassi americane a garantire sufficiente protezione dal controllo operato da autorità pubbliche degli USA sui dati trasferiti verso tale Paese, di cui alle rivelazioni di Snowden. L'autorità irlandese, però, aveva respinto il reclamo con la motivazione che la Commissione europea aveva già ritenuto adeguata la protezione dei dati personali offerta dagli Stati Uniti con la Decisione 2000/520/CE. L'interessato, in seguito, aveva, adito l'Alta Corte di Giustizia irlandese, che aveva disposto un "*rinvio pregiudiziale*" alla Corte di Giustizia europea della questione se una decisione della Commissione avesse l'effetto di impedire ad un'autorità nazionale di controllo di indagare sull'adeguatezza del livello di protezione offerto da uno Stato terzo e di sospendere, eventualmente, il trasferimento contestato dei dati. Il "*rinvio pregiudiziale*" consente ai giudici degli Stati membri, nell'ambito di una controversia della quale sono investiti, di interpellare la Corte in merito all'interpretazione del diritto dell'Unione o alla validità di un atto dell'Unione, per risolvere, poi, la causa conformemente alla decisione della Corte.

[14] In particolare dalla NSA (National Security Agency).

come una compromissione dell'essenza del diritto fondamentale del rispetto della vita privata".

Inoltre, la Corte ha stabilito che un'autorità nazionale garante della privacy, investita di una controversia, nel caso ritenga che una decisione della Commissione sia invalida, può, indipendentemente dall'esistenza di una decisione della Commissione che stabilisce che un paese terzo offre un adeguato livello di protezione dei dati personali:
(i) valutare, in piena indipendenza, se il trasferimento dei dati personali di un soggetto verso quel paese rispetta le norme comunitarie sulla protezione dei dati[15], nonché
(ii) rivolgersi ai giudici nazionali affinché, nel caso in cui anche questi abbiano dubbi sulla validità della decisione stessa circa il trasferimento, possano procedere ad un "*rinvio pregiudiziale*"[16] dell'oggetto della controversia dinanzi alla Corte di giustizia europea. Allo stesso titolo può agire direttamente l'interessato. Pertanto, nella sentenza si afferma che, in ultima analisi, è alla Corte che spetta il compito di decidere se una decisione della Commissione sia valida o no.

Infine, la Corte dichiara che la decisione della Commissione del 26 luglio 2000 priva le autorità nazionali di controllo dei loro poteri nel caso in cui una persona contesti la compatibilità della decisione "*Safe Harbour*" con la tutela della vita privata e delle libertà e diritti fondamentali delle persone.

Ai sensi della decisione suddetta, le autorità per la protezione dei dati (APT) degli Stati membri dell'UE hanno la facoltà, in specifici

[15] Si legge infatti nella sentenza: "*anche quando esiste una decisione della Commissione, le autorità nazionali di controllo, investite di una domanda, devono poter esaminare in piena indipendenza se il trasferimento dei dati di una persona verso un Paese terzo rispetti i requisiti stabiliti dalla Direttiva*".

[16] Il "rinvio pregiudiziale" consente ai giudici degli Stati membri, nell'ambito di una controversia della quale sono investiti, di interpellare la Corte in merito all'interpretazione del diritto dell'Unione o alla validità di un atto dell'Unione. La Corte non risolve la controversia nazionale. Spetta al giudice nazionale risolvere la causa conformemente alla decisione della Corte.

casi[17], peraltro non ancora esercitata, almeno fino al 2013, secondo la comunicazione della Commissione COM(2013) 847 final, di sospendere i trasferimenti di dati verso imprese certificate nell'ambito di Approdo sicuro e, quindi, possono esercitare un controllo "ex post" sull'applicazione dei principi "Safe Harbour", ma non un controllo "ex ante", formale, come pretende, invece, la Corte, seppure innescato da una segnalazione del soggetto dei dati all'autorità di protezione dei dati. Nella sentenza, pertanto, la Corte conclude pronunciandosi sull'invalidità della decisione 2000/520, sia per il mancato accertamento da parte della Commissione del grado di tutela dei diritti fondamentali della privacy (tra cui, trattamenti dei dati incompatibili con le finalità del loro trasferimento, od in eccesso rispetto da esso previsti, accesso ai propri dati da parte dell'interessato, accessibilità in sede amministrativa o giudiziale per ottenerne ad esempio la rettifica o cancellazione) equivalente a quello garantito dalla Direttiva, limitandosi essa solo ad esaminare il regime "Safe Harbour", sia per non avere la Commissione la competenza di limitare i poteri delle autorità nazionali di controllo. A seguito della sentenza in esame, l'autorità irlandese di controllo è tenuta a esaminare la denuncia del sig. Schrems con tutta la diligenza necessaria e, al termine della sua indagine, decidere se, in forza della direttiva, occorra sospendere il trasferimento dei dati degli iscritti europei a Facebook verso gli Stati Uniti perché tale paese non offra un livello di protezione dei dati personali adeguato.

5. Valutazioni in ambito comunitario della sentenza della Corte di giustizia europea e suoi effetti

La sentenza della Corte è focalizzata sulla illegalità della Decisione "Safe Harbour" della Commissione, ma anche tutte le altre Decisioni di adeguatezza da essa in precedenza disposte, includendo una disposizione che limita i poteri delle autorità di protezione dei dati

[17] Ad esempio accertamento da parte degli enti governativi degli USA di violazione dei principi Safe Harbour o mancata adozione di misure adeguate da parte degli stessi.

identica a quella prevista dall'art. 3 della Decisione *Safe Harbour*, sono giudicate illegali nella Comunicazione COM(2015) 566 final dell'11 novembre 2015 della Commissione, che, pertanto, in un'apposita Decisione disporrà la rimozione di detta limitazione. Oltre all'impatto dirompente sull'impianto normativo che disciplina i trasferimenti all'estero dei dati (artt. 25 e 26 della vigente direttiva corrispondenti agli articoli 40 e 41 dell'attuale proposta di Regolamento), la sentenza della Corte si caratterizza per la preminenza su interessi di business attribuita al diritto alla protezione dei dati personali, tra l'altro garantito dalla Carta dei diritti fondamentali dell'Unione Europea, e la missione di cui sono investite le autorità nazionali di controllo in forza della Direttiva.

Da questa sentenza discendono importanti conseguenze, tra cui inevitabilmente un aggiornamento dell'attuale sistema di Approdo sicuro e cambiamenti possibili del regime giuridico dei social network. Innanzitutto è da prevedere il proliferare dei casi di sospensione dei trasferimenti dei dati in USA sotto l'egida dei principi dell'Accordo "Safe Harbour". Essa avrà luogo ogni volta che il Garante della privacy in uno Stato membro, chiamato in causa da un'istanza di un soggetto di dati, accerti che il trattamento dei dati negli USA sia illecito – il che secondo logica dovrebbe accadere sempre, considerato che è emblematico il caso su cui si è pronunziata la Corte – nel senso di palese violazione della privacy, ossia, concretamente, di mancato rispetto di regole equivalenti a quelle europee. In tal caso, in attesa che venga istituito un nuovo valido Accordo", le società multinazionali potrebbero avvalersi di policy intra-gruppo vincolanti, che conservano la loro validità dopo la sentenza, che, una volta approvate dai Garanti della privacy, certificano la correttezza dei trasferimenti tra società del Gruppo (*Binding Corporate Rules*).

Il Working Party ex art. 29 della Direttiva 95/46/CE, organo consultivo indipendente in tema di privacy[18], nel suo parere del 16 ottobre 2015, commentando la sentenza della Corte di giustizia

[18] Il gruppo di lavoro è composto da rappresentanti delle Autorità europee garanti della privacy, della Commissione europea e dal Supervisore europeo per la tutela dei dati.

europea, scrive che è "assolutamente essenziale" per i Paesi dell'Ue adottare una posizione comune sull'implementazione della sentenza della Corte di Giustizia europea. Il succitato gruppo di lavoro sottolinea che la questione della sorveglianza massiccia e indiscriminata è un elemento basilare nell'analisi della Corte, in quanto da essa giudicata incompatibile con il quadro normativo dell'UE, che gli attuali strumenti di trasferimento dei dati non varrebbero a limitare o regolamentare. Pertanto, osserva il WP ex art. 29, la Corte stabilisce il fondamentale criterio in base al quale non saranno considerati 'sicuri' i trasferimenti verso Paesi terzi dove i poteri delle autorità Statali per accedere alle informazioni "*vanno oltre quello che è necessario in una società democratica*". Proprio per questo l'organo giudiziario avrebbe giudicato invalida la Decisione della Commissione 2000/520/CE che autorizzava il trasferimento dei dati oltreoceano, in quanto non avvalorata da un'ampia doverosa analisi delle leggi vigenti negli USA in materia di tutela dei dati e degli impegni internazionali sottoscritti dalle autorità statali di questo paese che escludesse ingerenze indebite delle autorità statali nella privacy dei cittadini. Dal canto suo, Il Working Party invita caldamente gli Stati membri e le istituzioni europee ad intavolare negoziati con le Autorità statunitensi per individuare soluzioni tecniche a dichiara che seguirà attentamente lo sviluppo delle procedure pendenti presso l'alta Corte di Giustizia irlandese a seguito della sentenza. Occorrerà a tale riguardo, scrivono i Garanti, pervenire alla stipula di un accordo al massimo livello e, quindi, intergovernativo che offra forti garanzie ai soggetti dei dati Ue. Stabilisce, inoltre, che nel periodo intercorrente la risoluzione del problema, le Autorità sulla protezione dei dati personali considereranno legittimo l'uso delle *Standard Contractual Clauses* e delle *Binding Corporate Rules*, ma eserciteranno comunque il loro potere di investigare singoli casi se riceveranno dei reclami. Il Gruppo di lavoro fa, poi, presente che se entro la fine di gennaio 2016 Europa e Stati Uniti non avranno trovato una soluzione 'appropriata', le summenzionate Autorità dell'UE adotteranno tutte le azioni "necessarie e appropriate", che potranno includere "azioni coordinate di enforcement". Nel frattempo ribadisce che "è chiaro che i trasferimenti dall'Unione europea verso gli Stati Uniti non possono più

essere inquadrati all'interno della *Safe Harbour decision*, e in ogni caso i trasferimenti che avvengono in base ad essa dopo la decisione della Corte di giustizia europea sono illegali". Occorrerà, pertanto, che le autorità europee di protezione dei dati, mettano in atto campagne pubblicitarie a livello nazionale, ad esempio mediante messaggi sui loro siti web, che forniscano ogni informazione utile sul nuovo sviluppo del regime "Safe Harbour" alle imprese che ne usufruiscono. Conseguentemente annuncia che incorreranno in sanzioni le aziende Usa che continueranno a importare, da fine gennaio 2016, dati europei secondo le vecchie invalide regole del Safe Harbour.

A margine di quanto sinteticamente riportato sopra in merito al parete espresso dal Working Party, non si può non ricordare che la decisione Approdo sicuro era stata adottata a seguito di un parere del medesimo Gruppo di lavoro, che ora, invece, condividendo la pronuncia della Corte, la dichiara illegale.

6. Prime ripercussioni della sentenza nel mondo della privacy

Il Commissario alla Giustizia Vera Jourovà ha dichiarato nella conferenza sulla privacy ad Amsterdam il 29 ottobre u.s. che la Commissione rispetta la sentenza della Corte e si conformerà ad essa e lo stesso dovranno fare tutti i portatori d'interesse. Pertanto nel breve periodo, aggiunge, non rimarrà alle imprese altra scelta se non ricorrere agli strumenti normativi alternativi previsti dalla direttiva 95/46/CE, ma che chiaramente occorrerà istituire un nuovo quadro regolamentare generale con gli Stati Uniti, comunque lo si voglia chiamare. Esprime soddisfazione che il *Judicial Redress Bill* sia passato alla Camera e si augura che presto possa essere approvato al Senato degli Stati Uniti. Ma allo stesso tempo fa rilevare le incertezze ancora sussistenti negli USA circa le limitazioni e le salvaguardie nell'accesso ai dati imposto per legge o per le finalità della sicurezza nazionale. Auspica, infine, un reciproco approfondimento delle culture sulla privacy nei due paesi, che concorra anche alla messa in atto di soluzioni pratiche e tecnologiche nell'area della *privacy by design*.

In Europa, le autorità di protezione dei dati hanno accolto favorevolmente la sentenza della Corte. Il Garante federale tedesco

addirittura saluta la sentenza come una pietra miliare per la tutela dei diritti fondamentali della privacy dei cittadini europei. Le predette autorità, considerata la sentenza della Corte e preso atto del parere del WP ex art. 29, hanno deliberato pronunciandosi sull'invalidità del Safe Harbour. In particolare il Garante italiano della privacy con il provvedimento del 22 ottobre 2015 ha disposto la caducazione dell'autorizzazione adottata dal medesimo in data 10 ottobre 2001 con deliberazione n. 36. Peraltro, il Ministero del commercio degli Stati Uniti ha pubblicato un avviso sul suo website (http://www.export.gov/safeharbor/), in cui afferma che continuerà a gestire il programma Safe Harbour, comprese le autocertificazioni sottoposte alla sua valutazione. Le autorità americane ribadiscono il concetto, già espresso in precedenza nelle varie sedi, che occorre procedere ad una riforma della normative sulla privacy che tenda in ogni paese ad un migliore bilanciamento tra la privacy e la sicurezza pubblica. Tra gli interventi legislativi interni, da compiere quanto prima, gli USA citano l'approvazione di una versione aggiornata dell'*ECPA (Electronic Communications Privacy Act)* che risale al 1986[19] [20], del *Law Enforcement Access to Data Stored Abroad* (LEAD) *Act* del 2015 e del *Judicial Redress Act*.

Dal canto loro, le multinazionali che offrono servizi tramite internet hanno dichiarato che, al di là dell'Approdo sicuro, continueranno ad assicurare una soddisfacente tutela dei dati. Ad esempio, la società Oracle, con riguardo alla fornitura di servizi di tipo *cloud*, ha dichiarato che provvederà ad immagazzinare i dati dei suoi clienti in *datacenter* ubicati in Europa e non altrove nel mondo, ma fa presente

[19] Uno degli emendamenti principali è costituito dal famigerato *USA Patriot Act* del 2001 (acronimo di *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* of 2001). Con l'approvazione del *USA Freedom Act* del 2 giugno 2015, che peraltro ha rinnovato la validità di alcune sue parti, scadenti nel 2015, fino al 2019, la sezione 215 è stata emendata per far cessare la raccolta di dati di comunicazioni telefoniche disposta dalla NSA, che, a seguito delle nuove norme, può ottenere informazioni esclusivamente su determinati utenti e solo con il permesso di una corte federale.

[20] L'ECPA è stato criticato negli USA in quanto verrebbe meno alla sua funzione di tutela delle comunicazioni degli utenti, soprattutto perché le norme sarebbero datate e non in sintonia con le modalità di condivisione, di memorizzazione e di utilizzo delle informazioni da parte dei consumatori ai giorni nostri.

che talune operazioni *cloud* possono richiedere l'accesso a risorse informatiche in altri paesi. La società precisa, peraltro, che l'accesso a queste risorse rispetta i requisiti imposti dalle norme della Direttiva 95/46/CE sui trasferimenti dei dati all'estero (art. 26) e non è legato in alcun modo al regime Safe Harbour, volendo sottolineare con ciò che la sentenza della Corte non ha alcun impatto sulla sua *policy* in materia di privacy. Oracle non ha fornito nessun dettaglio su come essa rispetta le norme UE sul trasferimento, ma è assai probabile che essa impieghi una forma diretta di clausole contrattuali, le cosiddette "*model contracts*", ossia SCC. A seguito della sentenza Schrems, alcune multinazionali come Amazon e Salesforce hanno pubblicizzato messaggi sui loro siti in cui viene dichiarato che i dati dei clienti trasferiti all'estero sono sicuri, perché esse hanno fatto uso del suddetto tipo di clausole. Anche la Microsoft, rivolgendosi ai clienti dei propri servizi (tra cui Azure Core Services, Office 365, Dynamics CRM Online, Microsoft Intune), ha assicurato che le SCC, che rispondono al modello fissato dall'Unione europea, e inserite fin dal 2011 nei contratti Cloud, costituiscono forme adeguate di tutela dei dati con riguardo al loro trasferimento verso paesi extraeuropei (tra cui gli USA), anche in assenza del Safe Harbour; e che nell'aprile del 2014 tali clausole sono state valutate adeguate anche dal Gruppo di Lavoro ex articolo 29. L'azienda di Redmond ha, altresì, richiamato l'attenzione sugli investimenti realizzati per la costruzione di oltre 100 *datacenter* in più di 40 paesi nel mondo in modo da trattare i dati in luoghi che siano il più vicino possibile a dove risiedono i clienti.

7. Valutazioni finali

La sentenza della Corte europea di Giustizia ha dichiarato giuridicamente invalida la decisione della Commissione istitutiva dell'Accordo "Safe Harbour". Il pronunciamento del Collegio non si riferisce al fatto che le imprese statunitensi certificate disattendono i 7 principi sottoscritti, né a verifiche di malfunzionamento delle procedure di attuazione dell'Accordo (come, invece, la Commissione ha rilevato a più riprese), ma si fonda sull'evidenza non confutabile che le condizioni imposte dalla legislazione degli USA prevalgono su

detti principi e sul livello di protezione dei dati. Pertanto, secondo la Corte, con la decisione di cui sopra la Commissione avrebbe mancato di considerare i criteri di adeguatezza di un paese terzo in merito al trasferimento dei dati di cui alla direttiva 95/46/CE. Al riguardo, si potrebbe obiettare che le basi giuridiche previste dalla legislazione americana che consente la raccolta e il trattamento su larga scala di dati personali trattati da società ubicate negli Stati Uniti sarebbero successive all'introduzione del regime di Approdo sicuro. In ogni caso, come nota la Commissione nella comunicazione COM(2013) 847, se è vero che il trattamento eccezionale di dati a fini di sicurezza nazionale, interesse pubblico o amministrazione della giustizia è previsto da Approdo sicuro, l'accesso su larga scala da parte dei servizi di intelligence ai dati trasferiti negli USA nel contesto di operazioni commerciali non era prevedibile all'epoca dell'adozione di tale regime.

A ben riflettere, poi, quanto deliberato dalla Corte non costituisce un "fulmine a ciel sereno" che colpisca in modo irreparabile e subitaneo gli scambi commerciali USA-Europa ed i relativi archivi dati costituiti via Internet. Occorre ricordare, infatti, che già nella Comunicazione della Commissione del 27/11/2013[21], come è stato evidenziato diffusamente in precedenza, vengono enfatizzate la scarsa trasparenza nelle *policies* di privacy delle imprese statunitensi aderenti all'Accordo e le insufficienti misure di controllo dell'attuazione delle norme da loro sottoscritte da parte delle Autorità di controllo degli USA, ossia Department of Commerce e Federal Trade Commission. L'Accordo *Safe Harbour* risulta, inoltre, già superato o perlomeno insufficiente alla luce del nuovo assetto normativo comunitario, come del resto le norme attuative del trasferimento dei dati; a tal riguardo, va osservato che l'emanando Regolamento destinato a sostituire la Direttiva 95/46/CE, conferma l'impianto normativo in materia di trasferimenti (e ogni altra decisione della Commissione ai sensi dell'art. 26.4) per un periodo massimo di cinque anni dalla sua entrata

[21] EUROPEAN COMMISSION, *Communication on the Functioning of the Safe Harbour from the Perspective of EU citizens and Companies Established in the EU*, 27 November 2013.

in vigore[22]. Infatti il mantenimento del comma 2 dell'art. 3 nella versione di cui sopra – che stabilisce che le imprese non europee che offrono beni e servizi ai consumatori europei, indipendentemente dall'applicazione o meno di una tariffa, o svolgono attività di monitoraggio del loro comportamento, sono tenute ad applicare *in toto* le norme di protezione dei dati vigenti in ambito europeo – pone non pochi interrogativi sulla compatibilità di quanto da esso prescritto con le Decisioni di adeguatezza attuate in tutti questi anni dalla Commissione. L'accordo Safe Harbour potrebbe allora configurarsi come uno strumento, seppure ancora perfettamente legale secondo lo Schema di Regolamento, che consentirebbe l'aggiramento delle norme europee per i dati trasferiti sui server americani, che l'accessibilità ad essi da parte del programma PRISM renderebbe ancora più eclatante, che, invece, in base all'art. 3(2) andrebbero applicate, secondo quanto affermato in un suo discorso[23] dalla vicepresidente della Commissione Reding, in maniera uniforme dal momento della raccolta dei dati alla loro cancellazione/rimozione.

D'altro canto rimane valido quanto riaffermato dagli USA e dalla UE nel documento sottoscritto il 19 marzo 2012 dal vicepresidente della UE e dal Segretario del commercio USA John Bryson circa il reciproco impegno a rafforzare l'Accordo Safe Harbour, in piedi fin dal 2000, ritenuto un punto di partenza imprescindibile per una maggiore interoperabilità dei sistemi normativo-regolamentare della privacy applicati nelle due sponde dell'Atlantico. Con riferimento al sistema di tutela dei dati vigente negli USA, il vicepresidente della UE ed ex Commissario della Giustizia Viviane Reding aveva a suo tempo ripetutamente ricordato alle Autorità preposte a detta tutela che le regole della privacy devono essere applicate indipendentemente dalla nazionalità dell'interessato ("*data subject*") e che applicare differenti standard a residenti e a non residenti, come difatti continua ad avvenire complice anche l'ombrello protettivo per l'industria

[22] *Amendment* n.ro 137 introdotto dal Parlamento europeo il 12 marzo 2014.
[23] V. REDING, "*Data protection reform: restoring trust and building the digital single market".* SPEECH/13/720 del 17/09/2013.

americana del Safe Harbour, non ha senso, quanto meno alla luce della natura aperta di Internet[24].

In conclusione la pronuncia della Corte impone una revisione del negoziato USA-UE in merito al trattamento dei dati dei cittadini europei trasferiti nei server degli USA, senza, peraltro, costituire un fondamento giuridico del quale ci si possa avvalere per destituire di validità legale a priori qualsiasi flusso di dati in detta direzione. Neanche è possibile la promozione di azioni giuridiche individuali o *class action* miranti alla cancellazione dei dati conservati nei suddetti server. E' quanto precisa la Comunicazione della Commissione COM(2015) 566 final del 11 novembre 2015. E', peraltro, *sub judice* il mantenimento dei dati già trasferiti prima della sentenza nei server statunitensi che è legato all'esito del caso che il Garante della privacy irlandese è chiamato a definire ora che la Corte di Giustizia UE, precedentemente chiamata in causa dalla Corte irlandese, ha espresso la sua pronuncia. Al riguardo però i Garanti europei hanno già annunciato che le indicazioni saranno unitarie. Si fa, altresì, rilevare che, nel caso di decadenza dichiarata dello stato di adeguatezza delle norme di tutela in USA a quelle comunitarie, per effetto dell'annullamento della Decisione Safe Harbour, laddove un utente, nell'aderire a servizi online, abbia accettato od accetti il trasferimento in USA dei suoi dati personali sulla base di clausole quali quelle dell'Accordo Approdo sicuro o di quelle standard oppure BCR, in deroga alle norme di diritto UE è da considerare legittimo il trattamento oltreoceano e, pertanto, è improbabile che il Garante nazionale della privacy possa ordinare la rimozione dei dati dal server americano.

La sopra richiamata comunicazione del 2015, tenuto conto che il trasferimento dei dati oltreoceano è strettamente connesso agli scambi commerciali USA-Europa, costituendo in termini più generali un motore dell'economia digitale a livello globale, giudica quale priorità chiave la sopravvivenza dell'Accordo Safe Harbour in un quadro più stringente di regole concordate tra le due Parti, di qua e aldilà dell'Oceano, che assicuri un'efficace continuità di protezione dei dati

[24] V. REDING, *Data Protection Day 2014: Vice-President Reding calls for a new data protection compact for Europe European Commission,* IP/14/70, 28/01/2014.

trasferiti. Senza trascurare il fatto che il Safe Harbour costituisce uno strumento la cui applicazione è ritenuta dalla Commissione nel documento citato, di più semplice impiego e assai meno onerosa, in termini di appesantimenti burocratici e di costi, rispetto agli altri precedentemente esaminati che sarà opportuno impiegare solo in un periodo transitorio. In sostanza la posizione della Commissione sull'evoluzione dell'Accordo, pure espressa in termini di neutra eleganza e prudenza, si potrebbe riassumere nella classica espressione di continuità monarchica: *"Morto il re. Viva il re!"*.

Nelle more di un rinnovato negoziato che conduca ad un Accordo Safe Harbour rafforzato, la Commissione raccomanda alle autorità nazionali di protezione dei dati il loro ruolo di custodi della salvaguardia dei diritti fondamentali degli interessati, agendo, in piena indipendenza, da supervisori dei trasferimenti dei dati dall'UE in paesi terzi. Nel negoziato aperto nel 2013 con il governo degli Stati Uniti gli USA, la Commissione aveva rivolto ad esso una serie di raccomandazioni, tra cui un monitoraggio ed un'imposizione più severa ed effettiva dell'applicazione nella prassi dei principi Safe Harbour da parte rispettivamente il Ministero del Commercio e la Commissione Federale del Commercio (FTC) degli Stati Uniti, una maggiore trasparenza per i consumatori per quanto riguarda i loro diritti alla protezione dei dati, una più facile e meno costosa possibilità di ricorso in caso di reclami e la limitazione dell'accesso ai dati e della loro raccolta da parte di una pubblica autorità, previsti dall'Accordo Safe Harbour, ai soli casi motivati in maniera stringente da esigenze di sicurezza nazionale ed esclusivamente in misura strettamente necessaria e proporzionata.

Nella comunicazione COM(2015) 566 final la Commissione rileva che sono stati compiuti notevoli progressi nell'avvicinare le opinioni di entrambe le parti su quasi tutti i suddetti punti critici di funzionamento dell'Approdo sicuro, salvo ad esempio quello dell'accesso e raccolta ai dati messi in atto da agenzie di intelligence. I suddetti organismi degli USA, dal loro canto, quasi a voler rispondere alla sentenza della Corte, affermano di aver fornito all'Unione Europea sufficienti garanzie a tale riguardo, ed un loro rappresentante ha dichiarato che negli ultimi due anni, con finalità di salvaguardia della privacy, sono state introdotte in sede normativa restrizioni

all'accesso ai dati personali nei confronti delle agenzie di intelligence statunitensi, di cui la Corte avrebbe dovuto tener conto. Questo importante annuncio è stato presentato per iscritto recentemente, a valle della sentenza della Corte, al Congresso degli Stati Uniti da Ted Dean, un "senior official" presso la FTC, che è il leader della delegazione americana che sta conducendo i negoziati ed uno degli artefici principali dell'Accordo Safe Harbour, che ha inoltre aggiunto che in USA il diritto alla privacy è ben tutelato dalla legge e lamenta che la Corte di Giustizia europea dimostri di dare scarso credito a tale livello di protezione. Entrambe le parti sulle due sponde dell'Oceano si mostrano fiduciose nel pervenire ad un accordo all'inizio del nuovo anno, ma prevedibilmente le modalità condivise di accesso ai dati personali online (post sui social media, tracciamento di ricerche di navigazione in Rete, informazioni tradizionali, tra cui quelle finanziarie, record di dati informativi personali) da riconoscere secondo limiti prestabiliti ad agenzie di intelligence nazionali, costituiranno un ostacolo non indifferente per il raggiungimento di un così rilevante obiettivo.

In ogni caso, quale che sia l'esito dei negoziati, non si avranno riflessi di nessun tipo sul TTIP (*Transatlantic Trust and Investment Partnership*), così come, in un ambito ben più generale, l'emanando regolamento sulla tutela dei dati, ormai in dirittura d'arrivo, non avrà alcun impatto su di esso. E' quanto sostenuto dalla Reding nel suo discorso del 17 settembre 2013, che sottolinea come la protezione dei dati sia un diritto fondamentale, che per sua natura è differente dalla tariffa di un bene o dalla schedulazione di un servizio, oggetto del TTIP. Invece, il suddetto regolamento costituirà, secondo la vicepresidente della Commissione, un pilastro del *Digital Sigle Market* garantendo la riservatezza e cybersecurity dei dati ed allo stesso tempo un suo completamento con l'implementazione del principio "*One continent, one law*", in concreto con la sostituzione di 28 leggi sulla privacy con un'unica legge –il Regolamento- fatta da non più di 90 articoli e valida dappertutto in Europa. Inoltre, questa legge unica sarà applicata allo stesso modo in ogni Stato membro dell'UE, grazie al mantenimento dei poteri delle autorità di protezione dei dati nel prendere decisioni individuali, ma anche alla pressione dei pari esplicata su di esse, che nel nuovo assetto normativo sarà

maggiore di prima, tenuto anche conto che i loro poteri saranno gli stessi in tutta Europa.

Con riguardo all'impatto sul TTIP, diversa è la posizione sull'altra sponda dell'oceano. Il segretario di stato del commercio Penny Pritzker ha sostenuto[25] che uno schema Safe Harbour è di importanza cruciale nei negoziati TTIP, perché senza di esso sarebbe difficile inserire i flussi dei dati in esso.

[25] Cfr. http://arstechnica.com/tech-policy/2015/10/fallout-from-eu-us-safe-harbour-ruling-will-be-dramatic-and-far-reaChing/

L'orizzonte di scelta del cyberconsumer tra consapevolezza e condizionamento

FABIANA DE FEO*

SOMMARIO: 1. Introduzione. – 2. Tecnologie digitali e nuovi percorsi del diritto. – 3. Modificazione antropologica e scambi senza accordo. – 4. "Fatti non foste a viver come bruti": l'"uomo di vetro" tra informazione e controllo.

1. Introduzione.

La riflessione su alcune articolazioni del dibattito internazionale contemporaneo sollecitato dalla virtualità elettronica ha indotto ad interrogarsi sull'attuale problematica della libertà di scelta del soggetto digitale. Partendo dall'analisi di alcuni aspetti dello status del nuovo consumatore e dell'impatto che le nuove tecnologie hanno avuto sul mercato, si tenterà di descrivere alcuni risvolti della trasformazione antropologica in atto. I processi di virtualizzazione delle dinamiche comunicative contemporanee hanno condotto ad una riconfigurazione della società dei consumi, che ha richiesto, e continua a richiedere, un'adeguata risposta normativa, capace di interpretare il mutamento epocale sortito dalla rivoluzione digitale.

Non si intende esprimere giudizi di valore sullo scenario emergente, difficilmente categorizzabile in paradigmi conoscitivi definiti, né di assumere posizioni radicali riguardo alle dicotomie costruite intorno al digitale, ma di affrontare le questioni relative ai pericoli determinati dal processo di digitalizzazione non ancorandosi a prospettive ontologicamente determinate, bensì cercando di ricostruire gli accadimenti così come si stanno verificando, considerati nella loro complessità e problematicità. Il consumatore contemporaneo è "espressione della storia, delle tante microstorie in cui si frammenta il vivere d'oggi […]. Un soggetto in costante evoluzione perché

* Università degli Studi di Napoli Federico II.

immerso nel grande flusso del cambiamento (sociale, tecnologico, economico) che penetra anche nei più reconditi pertugi della nostra esistenza"[1], il protagonista di una profonda rivoluzione tecnologica ancora in atto, la quale ha prodotto una cultura dell'informazione che, come osserva Jean Baudrillard, costruisce un'*estetica* della "simulazione"[2], dove la differenza tra reale e immaginario, realtà fisica e realtà virtuale, vero e falso tende a svanire.

La simulazione viene intesa non come una fedele replica degli artefatti e come loro infinita riproducibilità (processi che hanno caratterizzato la modernità), ma come ingresso in un'area in cui i modelli di simulazione si sostituiscono al mondo reale. Nella postmodernità ormai esiste una continua promiscuità tra virtuale e reale, poiché alla luce dei vecchi paradigmi gran parte delle esperienze sembra lontana dalla concretezza dei processi materiali. "La straordinaria velocità con cui negli ultimi decenni il progresso ha trasformato i luoghi e i codici dell'interazione ha provocato una diffusa condizione di spaesamento, se non addirittura di inquietudine"[3]. Nella società della computerizzazione, come tiene a definirla uno dei più autorevoli teorici della postmodernità, Jean Francois Lyotard[4], ogni categorizzazione diviene vana, il tempo si frantuma in un'infinita molteplicità di presenti in cui si smarrisce la prospettiva storica, e lo spazio, con lo sviluppo della tecnologia satellitare, delle fibre ottiche e della cablatura sotterranea, si smaterializza; l'ubiquità nonché la simultaneità abbandonano la sfera metafisica per rientrare nel campo della consueta dimensione operativa umana. Si è di fronte a una galassia elettronica che

[1] G. FABRIS, *Il nuovo consumatore verso il postmoderno*, Franco Angeli, Milano, 2003, p.13.

[2] Basti il rinvio a J. BAUDRILLARD, *La società dei consumi. I suoi miti e le sue strutture*, Il Mulino, Bologna, 2010. Il consumo è, per Baudrillard, un processo di comunicazione che trasforma gli oggetti in simboli di un codice inteso a classificare e contrassegnare. All'autore inoltre si devono alcune parole chiave del linguaggio contemporaneo, tra cui si annoverano, tra le altre, quelle di "simulacro" e "iperrealtà".

[3] A. PUNZI, *Dialogica del diritto. Studi per una filosofia della giurisprudenza*, Giappichelli, Torino, 2009, p. 263.

[4] J.F. LYOTARD, *La condizione postmoderna. Rapporti sul sapere*, Feltrinelli, Milano, 2002.

ricostituisce il modello del nuovo "villaggio globale"[5] in cui i rapporti si instaurano secondo la logica reticolare del network. "È in questo *Nuovissimo Mondo*, che si è presentato, agli occhi dell'inesperto, con tutta la meraviglia che destano nuove e sconosciute terre, che si trova a fare i suoi acquisti il consumatore postmoderno. Un luogo ove tutto è lecito perché non governabile, ove la propria presenza appare esposta ad ogni intrusione da parte di chi ne ha i mezzi e i poteri"[6]. In questo trasformato panorama mediatico nasce l'esigenza di creare una relazione duratura con il consumatore, che appare sempre più guidato nelle sue scelte dalle "emozioni che battono sul tempo la ragione"[7].

Emergono nuove discipline: il marketing tradizionale, che seguiva un percorso lineare utilizzando strategie di seduzione del consumatore, cede il passo al neuromarketing, che segna un percorso circolare, partendo dal consumatore, comprendendone i meccanismi cognitivi e modellandosi sui suoi bisogni per cercare di soddisfarli. L'obiettivo è quello di insinuarsi nella mente degli internauti, di decifrare i loro comportamenti, i loro gusti e in particolar modo i loro desideri: le neuroscienze potrebbero schiudere "le porte ad una rideclinazione in chiave info-genetica del *conosci te stesso* socratico, dunque, l'uomo non dovrebbe temere di guardare in se stesso e nel proprio cervello, né disperare nella possibilità di fare un uso prudente dei risultati di tale esplorazione"[8]. Il descrivere l'evoluzione dello status del consumatore, ora più appropriatamente definito *cyberconsumer*, è però solo lo spunto per compiere una riflessione più ampia sull'influenza che le nuove tecnologie hanno avuto sulla libertà di scelta dell'uomo in generale, invadendo tutti i campi e non solo quello del mercato. È in atto una lenta e complessa trasformazione che

[5] Il "villaggio globale" è il fortunato ossimoro inventato da Marshall McLuhan per descrivere la contraddizione che segna l'epoca contemporanea. I due termini dell'enunciato sono, infatti, l'uno l'antitesi dell'altro: la parola "villaggio" indica una piccola comunità mentre il termine "globale" sta a significare l'intero pianeta. Si veda M. MCLUHAN, *Gli strumenti del comunicare*, Il Saggiatore, Milano, 2008.

[6] Si veda F. ROMEO, *Ars libertatis: esercizi intellettuali in cerca di nuovi spazi giuridici per le libertà politiche*, in *Diritto, Economia e Tecnologie della Privacy*, n.1, 2011, p. 79.

[7] A. PUNZI, *Dialogica del diritto*, cit., p. 314.

[8] *Ivi*, 312.

segna il passaggio da un consumatore "spettatore di azioni concertate altrove"[9] al cyberconsumatore[10], da un sistema di produzione centrico ad uno copernicano, che vede il consumatore al centro del sistema[11]. Non c'è dubbio che la tecnologia sia un attivatore di rivoluzioni e cambiamenti ed è evidente che il diritto debba adattarsi alla ridefinizione dello spazio comunicativo.

2. Tecnologie digitali e nuovi percorsi del diritto.

Non retorica appare la riflessione circa l'incidenza della tecnologia informatica e telematica sul diritto. "Al cospetto di un orizzonte così configurato, in cui si corre il rischio di veder garantita la sicurezza del consorzio sociale solo a fronte di una rinuncia delle libertà fondamentali, occorre verificare l'assunto secondo cui il diritto oggi sarebbe condannato allo status di ancella della tecnica"[12]. Appare necessario considerare le rilevanti implicazioni della "profezia nichilistica dell'asservimento del *nomos* alla *techne*", che renderebbe il diritto "mero strumento di controllo e normalizzazione della sicurezza e dell'efficienza della vita sociale"[13].

A causa dell'inerzia, del ritardo o comunque dell'inadeguatezza dell'intervento del Legislatore, la rete delle relazioni, anche commerciali, operanti su Internet è stata a lungo considerata uno spazio "vuoto di diritto". Essendosi verificato un radicale cambiamento di ciò che concerne i contenuti, la forma e le parti contraenti, l'informatica è diventata un indispensabile strumento delle operazioni giuridiche, trasformando dall'interno vaste aree del diritto e rendendo pienamente legittima l'espressione *diritto dell'era digitale*.

[9] G. ALPA, *I diritti dei consumatori e il Codice del consumo nell'esperienza italiana*, in Contratto e impresa. Europa, Volume 11, n.1, 2006, p. 3.
[10] Per un approfondimento delle tematiche relative alla figura del cyberconsumatore e ai suoi mezzi di tutela si veda A. LISI, *I contratti di Internet: sottoscrizione, nuovi contratti, tutela del consumatore, privacy e mezzi di pagamento*, Utet giuridica, Assago, 2006, pp. 180 ss.
[11] G. FABRIS, *Il nuovo consumatore: verso il postmoderno*, cit., p. 22.
[12] A. PUNZI, *Dialogica del diritto,* cit., p. 264.
[13] *Ivi*, p. 276.

La quasi totalità della disciplina consumeristica italiana è, infatti, di derivazione comunitaria[14] e consiste in atti di recepimento di direttive europee, peraltro attuate, non di rado, con molto ritardo rispetto ai tempi previsti. Internet e l'*e-commerce* hanno rappresentato il terreno ideale per l'affermazione di uno *jus in stadio nascendi*[15]: sempre più urgente è diventata la definizione delle attività in rete nonché delle consuetudini di *netiquette*, cioè di accordi spontanei sulle regole di condotta corretta nel ciberspazio come fonte reale di nuovo diritto.

[14] Per una sintetica ricostruzione del percorso normativo comunitario in relazione alla nascita dell'*e-commerce* si veda S. SICA, A.G. PARISI, *La tutela del consumatore nel contratto on-line*, in A.M. GAMBINO, (a cura di) *Rimedi e tecniche di protezione del consumatore*, Giappichelli, Torino, 2011, pp. 35-36: "Alla luce della prevedibile insufficienza di strumenti di regolamentazione, tanto il legislatore comunitario che il legislatore italiano hanno provveduto ad emanare provvedimenti miranti alla soluzione delle principali problematiche connesse *all'e-commerce* ed alla tutela del consumatore. Il summit di Ottawa del 1998 ha posto in particolare rilievo l'importanza del commercio elettronico, con riferimento al suo successivo sviluppo e ha sottolineato a tal fine l'assoluta necessità di rafforzare la fiducia degli utenti e dei consumatori attraverso la predisposizione di norme efficaci, tali da tutelare la riservatezza e garantire la protezione dei consumatori e la sicurezza delle tecnologie utilizzate. La direttiva 2000/31/CE, che rappresenta la disciplina di riferimento, ha inteso predisporre uno spazio privo di frontiere nazionali per i servizi della società europea dell'informazione, tenendo conto anche della necessità di consolidare il dialogo e la cooperazione internazionale in tema di regolamentazione dell'*e-commerce*. Il provvedimento comunitario, in accoglimento degli input della Conferenza di Ottawa, prevede innanzitutto, a garanzia della trasparenza dei rapporti, una serie di obblighi informativi a carico del prestatore di servizi elettronici. Un'apposita sezione è dedicata alle comunicazioni commerciali con disposizioni che operano sul piano informativo e sul versante della tutela della privacy. La parte centrale del provvedimento, invece, è rappresentata dalle disposizioni sui contratti conclusi per via elettronica. A tal proposito la nuova disciplina prevede, in primo luogo, l'impegno degli Stati di consentire l'efficacia giuridica dei contratti negoziati e conclusi per via telematica (eccezione fatta per una serie di deroghe espressamente previste come i contratti che implicano l'intervento di un notaio o una registrazione pubblica, nonché i contratti in materia di diritto di famiglia e successione). In secondo luogo si provvede ad indicare le informazioni che devono essere fornite al contraente da parte del proponente (relative, in particolare, alle fasi contrattuali e all'archiviazione dell'atto), nonché ad individuare in termini certi modalità e tempi di conclusione del contratto".

[15] *Ivi*, p. 30.

Il processo di globalizzazione ha generato una riconfigurazione delle coordinate spazio-temporali, nonché rilevanti trasformazioni in ambito giuridico. Le potenzialità dell'intelligenza connettiva hanno condotto a una "presenza ipertrofica del presente che passa progressivamente dall'essere una deperibile parentesi, racchiusa tra passato e futuro, al porsi come una dimensione temporale che diventa sempre più protagonista"[16]. Sul piano istituzionale si rinuncia all'ufficialità dei procedimenti, alla redazione di nuovi codici nonché all'eredità consegnataci dai padri costituenti. La dimensione transnazionale e l'era del "presente esteso" mettono in evidenza la discrasia tra diritto scritto e "diritto vivente", mentre si indebolisce il tradizionale "primato della legge, un tempo incontrastata signora e prima attrice della scena giuridica"[17]. All'ipertrofica produzione legislativa si contrappone un palese impoverimento qualitativo: la legge perde, infatti, il suo primigenio carattere decisionistico a causa di una contaminazione con inedite, fluide forme giuridiche.

Nell'orizzonte di quello che viene definito "*panopticon* elettronico"[18] si verifica una radicale ricostruzione della relazione tra

[16] M.R. FERRARESE, *Il diritto al presente. Globalizzazione e tempo delle istituzioni*, Il Mulino, Bologna, 2002, p. 65.
[17] *Ivi*, p. 66.
[18] Il progetto architettonico del panopticon è teorizzato da Jeremy Bentham e rappresenta la forma paradigmatica del potere disciplinare. Il principio motore della struttura è lo *sguardo*: una costruzione ad anello sovrastata da una torre centrale, attraverso una calcolata economia degli spazi, assicura la massima visibilità. Il sorvegliante, dall'alto della sua posizione schermata dalle persiane, senza bisogno di muovere un passo, può tenere sotto controllo tutti. La stessa scelta del termine panopticon ha un significato evocativo, indicando il luogo ove tutto è visto (cfr. J. BENTHAM, *Panopticon ovvero la casa d'ispezione*, Marsilio, Padova, 2002). La struttura panottica benthamiana è ripresa da Michel Foucault che la considera un modello che va oltre la matrice carceraria e che rappresenta perfettamente il concetto di sorveglianza costante (cfr. M. FOUCAULT, *Sorvegliare e punire. Nascita della prigione*, Einaudi, Torino, 1975). Un ripensamento della tetra allegoria architettonica, resosi necessario con l'avvento delle tecnologie digitali, è operato David Lyon, che arriva a parlare, a giusto titolo, di *panopticon elettronico*, un dispositivo moderno che realizza una *dataveglianza* individuale e di massa, permettendo di riunire all'interno di una sola tecnologia le funzione del potere, perfettamente in linea con l'analisi foucaultiana (cfr. D. LYON, *L'occhio elettronico. Privacy e filosofia della sorveglianza*, Feltrinelli, Milano, 1997).

diritto e territorio che mette fortemente in crisi la realtà tradizionale dello Stato-nazione. Il concetto di confine geografico tende a vanificarsi e i luoghi perdono la capacità di originare nei soggetti il senso di appartenenza alle realtà socio-culturali nonché di attribuire loro specifiche configurazioni identitarie[19]. Occorre considerare che anche il diritto ha fondamento negli atti primordiali di occupazione e ripartizione della terra. Come osserva Carl Schmitt, l'occupazione della terra costituisce all'esterno, nei confronti di altri popoli, e all'interno, con riguardo all'ordinamento del suolo e della proprietà entro un territorio, l'archetipo di un processo giuridico costitutivo[20]. Questo atto originario viene interpretato dal filosofo tedesco[21] come evento storico e come categoria logica che determina una forma spaziale da cui discende ogni altro istituto e criterio di diritto. "La terra è, nel linguaggio mitico, la madre del diritto. Così la terra risulta legata al diritto in un triplice modo. Essa lo serba dentro di sé, come ricompensa del lavoro; lo mostra in sé, come confine netto; infine lo reca in sé, quale contrassegno pubblico dell'ordinamento"[22]. L'occupazione della terra, secondo l'autore, costituisce l'originario titolo giuridico alla base del diritto; il *nomos* indica "l'immediatezza di una forza giuridica non mediata da leggi, è un evento storico costitutivo, un atto di legittimità che solo conferisce senso alla legalità della mera legge"[23].

Per Schmitt le successive regolamentazioni, scritte e non scritte, si alimentano dalla misura interna di un atto "costitutivo e ordinativo in senso spaziale"[24]. Ordinamento e localizzazione, *Ordnung e Ortung*, coincidono appieno: la superficie terrestre occupata, resa individua dai confini, unita verso l'esterno e l'interno, si fa così luogo, spazio costitutivo e principio di ogni diritto. Il diritto è tutt'uno con la determinazione spaziale di un popolo. Sulla scorta delle riflessioni schmittiane ci si interroga su quale sia il ruolo del diritto rispetto

[19] Cfr. Z. BAUMAN, *Dentro la globalizzazione. Le conseguenze sulle persone*, Laterza, Roma-Bari, 1998, p. 119.
[20] C. SCHMITT, *Il nomos della Terra*, Adelphi, Milano, 1991, p. 25.
[21] *Ivi*, pp. 19-20.
[22] *Ibidem*.
[23] *Ivi*, p.63.
[24] *Ivi*, p. 70.

all'incedere del capitalismo contemporaneo, che confonde luoghi e dissolve confini. La questione viene alimentata dal prezioso contributo che Natalino Irti offre al dibattito interno alla cultura giuridica e filosofica italiana circa il rapporto tra diritto, tecnica ed economia. L'autore si chiede se "l'economia stia prima e se il diritto venga dopo: la prima è la perenne natura, il secondo, la mutevole e incerta storia degli uomini"[25]. Di fatto qualsiasi descrizione di economie naturali, fondate sul godimento collettivo di beni e sullo scambio di merci, si ritrova nella necessità logica di postulare forme ed istituti giuridici. Basti pensare che il mercato presuppone la proprietà privata dei mezzi di produzione e la tutela degli accordi. È lo stesso Irti che afferma che: "gli accordi, che non vogliono consegnarsi alla labile valutazione degli interessi individuali, vengono tutelati dall'esterno. Questa esternalità è ciò che propriamente segna l'aurora del diritto […], l'appello al terzo che ha il potere di pronunciare la parola del diritto nel caso concreto"[26]. La funzione conformatrice del diritto consiste proprio nel dare forma agli eventi esterni o nel costituirli come fatti giuridici. Il mercato è, come sottolinea Irti, "*locus artificialis*, ossia fatto con l'arte del legiferare. Non è il mercato ad esprimere dall'interno il proprio diritto, ma il diritto dall'esterno che lo costituisce e che lo conforma"[27]. Occorre quindi in definitiva un diritto che sia al passo con i tempi, che si adegui ai cambiamenti sociali e non resti intrappolato in vetusti meccanismi non più aderenti ad una realtà in costante evoluzione. È apparso quindi necessario l'intervento del Legislatore al fine di adeguare una normativa ormai obsoleta a nuove fattispecie generate dallo sviluppo tecnologico. Si è rivelata altresì opportuna un'attività di interpretazione estensiva, che, in assenza di organici interventi legislativi, consenta di adeguare l'ambito di operatività delle tradizionali categorie giuridiche alle nuove forme di aggressione telematica dei beni giuridici oggetto di protezione, tenendo costantemente in debito conto i principi di legalità e tassatività della fattispecie legale. In una prima fase non si è

[25] N. IRTI, *Il diritto e il mercato*, in AA.VV (a cura di), *Il dibattito sull'ordine giuridico del mercato*, Laterza, Roma-Bari, 1999, p. 8.
[26] *Ivi*, p. 11.
[27] *Ivi*, p. 17.

consentito al contratto informatico di essere collocato nella teoria generale del contratto, non essendo pensabile che i meccanismi contrattuali si svolgessero tra entità inanimate o non autonome, ma nella fase successiva si è tentato di ricondurre le fattispecie derivanti dal contratto informatico all'interno di categorie dogmatiche tradizionali, con conseguente mutamento di approccio nei confronti delle tecnologie digitali.

Occorre capire il valore da attribuire all'attività svolta in rete, passaggio essenziale per mettere ancora in luce le differenze o i punti in comune delle modalità di formazione dell'accordo telematico rispetto alle disposizioni del Codice Civile. Sarebbe, infatti, illusorio coltivare la pretesa di avere oggi a disposizione una regolazione piena, esaustiva ed efficace rispetto a un fenomeno così complesso, poiché, per fortuna o purtroppo, i problemi nascono spesso dalla prassi e talvolta dalla stessa regolamentazione[28]. La distanza tra la realtà regolamentata e quella non regolamentata è notevolmente aumentata, generando un ritardo assai forte nella disciplina di fenomeni rilevanti.

3. Modificazione antropologica e scambi senza accordo.

Il mercato globale che attualmente si svolge in rete mostra una realtà sociale ove la tecnologia configura e governa il rapporto tra i contraenti, con l'effetto, come osserva Irti, di dare vita a nuove figure che operano nel commercio, sino a segnare "il declino dell'*homo loquens*"[29], progressivamente sostituito dall'*homo videns.* Questa "modificazione antropologica"[30] ha rappresentato, secondo Giovanni Sartori, una regressione, un'atrofizzazione intellettuale e un'incapacità

[28] Non è casuale che la storia del commercio elettronico venga descritta come un "alternarsi di picchi di entusiasmo e di profonde disillusioni". G. BELLANTUONO, *Asimmetria informativa e razionalità limitata nei mercati elettronici*, in G. PASCUZZI (a cura di), *Diritto e tecnologie evolute del commercio elettronico*, Cedam, Padova, 2004, p. 13.

[29] N. IRTI, *Norma e luoghi. Problemi di geo-diritto*, Laterza, Roma-Bari, 2006, p. 173.

[30] G. SARTORI, *Homo videns. Televisione e post- pensiero*, Laterza, Roma-Bari, 1997, p.13.

di distinguere il virtuale dal reale e il vero dal falso. La conseguenza di questa involuzione è la sempre più crescente incapacità del soggetto di esercitare un'autonomia decisionale, che, per traslato, significa perdita della libertà e del libero arbitrio.

Diventa utile l'analisi compiuta da Paolo Spada, che muove da una distinzione radicale tra la tradizionale vetrina, ormai da tempo superata, e la vetrina virtuale della rete: da una parte lo studioso esamina la figura dell'*uomo consumatore che guarda*, cercando le merci che lo interessano mediante l'esercizio di uno sguardo attirato dagli oggetti concreti; dall'altra descrive la figura *dell'uomo consumatore che naviga* nelle reti telematiche e che compie la ricerca delle merci congetturando. Entrambe le figure si distinguono nettamente in relazione alle attività che le qualificano. La prima cerca esercitando lo *sguardo*, che, rispetto alla *vista*, possiede un surplus di qualità, e che, realizzando un'attività selettiva, segnata dall'originalità creativa e dalla non fungibilità, non si riduce al mero vedere. La seconda, quella dell'uomo che cerca congetturando, si lascia condurre, durante la navigazione, attraverso itinerari precostituiti dalla successione non scelta dei luoghi o, per dirla con Marc Augé, dei "nonluoghi"[31] che invadono la vista nonché dei siti incontrati: se nel consumatore che cerca con lo sguardo domina il momento della selezione, nel navigatore telematico, che cerca congetturando, domina invece la casualità dell'apparire delle immagini e la molteplicità in movimento delle icone, le quali tracciano un percorso non scelto dal cibernauta secondo un ordine progettato, ma in continua formazione, secondo il prodursi non anticipabile delle connessioni dettate dall'interattività. L'uomo produce la tecnologia, la quale, "a sua volta, lo produce e lo determina"[32], come è dimostrato dalla struttura antropologica corrispondente al *navigare congetturando*, che rende i consumatori non "più padroni del proprio sguardo su oggetti materiali esposti in uno spazio fisico o in spazi fisici consecutivi sulla linea del tempo", ma acquirenti che "si imbattono in oggetti che altri hanno

[31] M. AUGÉ, *Nonluoghi. Introduzione a una antropologia della surmodernità*, Elèuthera, Milano, 1993.
[32] P. SPADA, *Domain names e dominio dei nomi*, in "Rivista Diritto Civile", 2000, p.727.

collocato in un reticolo immateriale nel quale l'unica bussola è un'attività di tipo congetturale"[33]. Nel passaggio dall'acquisto nel grande magazzino a quello nelle reti, si avverte, come direbbe Irti, un profondo cambiamento, quasi una rivoluzione dei rapporti di scambio. Il sistema delle immagini rende presenti le cose assenti: l'*homo videns* prende perciò il posto dell'*homo loquens*. L'immediatezza sensoriale della figura subentra alla mediazione della parola, le cose non sono più sapute, ma vedute. Se l'*homo loquens* è colui che ricorre al sapere collettivo della lingua, l'*homo videns* è colui che percepisce, con l'immediatezza dell'occhio, la figura stessa delle cose[34]: "la parola *offre*, la cosa *si offre*; la parola evoca l'assente, la cosa è presente; la parola, [che ha un contenuto teoretico che l'occhio non può avere], chiede di essere capita, la cosa di essere percepita con la vista"[35]. L'immagine prende il posto della parola sopprimendo il dialogo e in questo modificato contesto il silenzio domina gli scambi, cosicché non si esige più la parola oppure la si riduce da atto dialogico ad atto informativo. È negli schermi dei computer che si riconosce il primato dell'immagine: non più parole che, conoscendo le cose, le denotano e le rappresentano e neppure più le cose nella loro fisicità, ma le immagini delle cose laddove queste da lontane diventano vicine. Se nei grandi magazzini le cose presenti attendono di essere scelte, nel ciberspazio la rappresentazione di cose assenti spesso invade la vista e l'espressione delle preferenze avviene selezionando la loro immagine. Traducendosi il tutto in pura visibilità, non è più l'individuo ad andare verso le cose, ma sono queste ultime, fermate in immagini, ad andare verso il soggetto, il quale, come sottolinea Irti, "non più *proferisce* parole, ma *preferisce* immagini di cose"[36]. L'uomo che lascia la parola, "perde e oblia la propria identità storica"[37], poiché la tecnologia telematica determina la creazione di un universo impalpabile, di un'astratta iperrealtà[38] che svuota le cose di storicità e

[33] *Ivi*, p. 731.
[34] *Ibidem.*
[35] N. IRTI, *Norma e luoghi*, cit., p. 173.
[36] *Ivi*, p.178.
[37] *Ibidem.*
[38] Non è più possibile costruire l'immaginario a partire dai dati del reale: la produzione, anzi la sovrapproduzione virtuale di oggetti, ideologie, segni, e la

territorialità. Sarebbe forse più opportuno correggere il famoso " in principio era Verbo" con "in principio era Immagine"[39], verbo che ha lasciato al silenzio delle immagini il mondo degli scambi. L'utente crede di chiedere ciò che desidera, ma in realtà desidera ciò che altri hanno deciso per lui. Si può constatare, così, che le tecnologie, costituendo un sistema pensante, "non sono servi obbedienti, ma padroni dispotici"[40]. Il consumatore appare quindi l'espressione di un'epoca ormai radicalmente ridelineata: in prima analisi, cogliendo la sua metamorfosi, lo si è definito uomo *topologico*, soggetto cioè legato ai nuovi topoi, i non luoghi, che caratterizzano l'ambiente telematico e ne costituiscono il substrato in cui egli si trova a operare. Se, come sostiene Irti, il consumo "nega la cosa come tale, la nientifica, la sospinge nel buio del non essere"[41], la postmodernità, che si riconosce e si rispecchia nell'idea dell'*in fieri*, ossia del giungere delle cose dal nulla e del loro ritornare nel nulla, ha il consumatore tra i principali interpreti. Ne *Il salvagente della forma*, in cui Irti identifica il consumo con un atto di violenza che esaurisce beni materiali e immateriali, mirando a determinare "un vuoto subito colmato e subito riaperto"[42], il consumatore, il quale usa, logora e distrugge le cose, rappresenta il "polo della distruzione", un'espressione paradigmatica del nichilismo.

4. "Fatti non foste a viver come bruti": l'"uomo di vetro" tra informazione e controllo.

Laddove un tempo il consumatore costituiva un antagonista debole del professionista, attualmente il cyberconsumatore, a differenza del suo antesignano, afferma il proprio ruolo, essendo in grado, grazie alla rete, di ricercare informazioni commerciali, confrontare prezzi e

riproduzione interminabile di ideali, immagini, sogni generano un processo di iperrealizzazione, che si dispiega in una simulazione indefinita. Si veda J. BAUDRILLARD, *La trasparenza del male*, SugarCo, Milano,1991, pp. 9-10.

[39] G. SARTORI, *Homo videns*, cit., p. 15.

[40] *Ibidem*.

[41] N. IRTI, *Il salvagente della forma*, Laterza, Roma-Bari, 2007, pp. 70-71.

[42] *Ibidem*.

servizi nonché cogliere offerte di imprenditori telematici[43]. È la realtà della stessa rete che induce a chiedersi se si sia effettivamente liberi di scegliere che cosa acquistare. La risposta va cercata analizzando un campo in rapido sviluppo, particolarmente interessante, quello del marketing diretto, l'insieme delle strategie, cioè, che non pubblicizzano un prodotto rivolgendosi ad un insieme indeterminato di persone, ma che indirizza l'offerta verso ogni singolo potenziale acquirente. Affinché tale operazione riesca è necessario conoscere i meccanismi psicologici, i gusti, le abitudini, le preferenze di ognuno, esercitando un tipo di condizionamento che, sulla base di informazioni individualizzate[44], influenza potentemente le scelte dei fruitori. Come osserva Francesco Romeo: "*oggi si è più refrattari ai condizionamenti, o si crede di esserlo, ma nuovi e potenti mezzi, tecnici e scientifici, permettono un'intrusione più pressante e selettiva nelle scelte individuali. Si deve necessariamente cambiare atteggiamento nei confronti di noi stessi e degli altri, imparare ad avere meno fiducia nelle nostre capacità di valutare coscientemente e di decidere, di essere capaci di non farci influenzare. Ognuno di noi è sensibile, in modo solo parzialmente differente, agli stimoli culturali esterni e da questi unitamente alle sue caratteristiche genetiche dipenderanno comportamento e scelte. Controllabilità empirica, invece di fede ed emozione, nonché evidenza invece di autorità,*

[43]Cfr. V. ARISTEI STRIPPOLI, *Le esigenze del cyberconsumatore nell'e-commerce*, in *Computer Law Informatica e diritto*, http://www.computerlaw.it/entry.asp?ENTRY_ID=53.

[44] Attualmente un'importante risorsa economica è rappresentata dalle informazioni degli individui, la cui capillare captazione è stata resa possibile attraverso le tecnologie digitali. Il passo successivo è stato l'utilizzazione di sofisticate tecniche di profilazione dei soggetti, operazione consistita nel rivelare le connessioni abituali dei cibernauti, i loro acquisti specifici e i loro bisogni, messi in luce dai siti visitati. I cosiddetti cookie (informazioni memorizzate sullo hard drive del navigatore) rappresentano un'ampia capacità di tracciamento per le imprese che vogliono sfruttare i dati relativi ai consumatori. Essendo le transazioni registrate, i potenziali clienti, spesso inconsapevolmente, lasciano *scie di tracce elettroniche*, assunte come indici di interessi che possono essere sfruttati commercialmente (in tema di informativa e di acquisizione del consenso si veda il provvedimento n. 229 dell'8 maggio 2014 assunto dal Garante della privacy).

tradizione e rivelazione potranno servirci da guida nella nostra autodeterminazione"[45].

Si può notare come l'influenza delle tecnologie digitali abbia potuto far dubitare della libertà di scelta di ogni soggetto, sempre più inconsapevolmente coartato. Spesso senza che gli individui se ne rendano conto la loro libertà viene sottoposta a continui condizionamenti. Questo è forse il prezzo da pagare del progresso, un progresso che consente in ogni istante di essere informati su tutto, di acquistare prodotti rimanendo comodamente a casa, conquistare il dono dell'ubiquità, ma che per contro rende tutti sempre più sorvegliati, seguiti, tracciati. "Che lo voglia o no, l'individuo postmoderno avverte sempre, accanto e intorno a sé, la presenza degli altri. Seguito nei suoi movimenti, conosciuto nelle sue scelte, scrutato nel suo lato esteriore ed interiore, egli sente di non essere mai solo: avverte l'inquietante sensazione di essersi trasformato in un flusso di informazioni"[46]. L'obiettivo del monitoraggio, ormai tipico della società contemporanea, permette, tramite un sistema informatico, di elaborare categorie entro le quali suddividere gli individui cercando di carpirne gusti, preferenze, inclinazioni e abitudini. La sorveglianza tradizionale, che ha segnato il Ventesimo secolo, era di fatto limitata a luoghi specifici: l'individuo era osservato solo in spazi definiti, quali prigioni o fabbriche, e i dati personali erano registrati soltanto su supporti cartacei e quasi esclusivamente utilizzati per finalità burocratiche[47]. Il sistema computerizzato ha dato luogo a una rete di connessioni più fitte rispetto a quelle realizzabili attraverso la documentazione cartacea, non più con il mero intento di immagazzinare dati, ma perseguendo il fine di prevederne i flussi futuri.

Particolarmente efficace si rivela la definizione che Antonio Punzi, in *Dialogica del diritto. Studi per una filosofia della giurisprudenza*, offre del dato, considerandolo come "un'impronta lasciata dal cammino dell'individuo, una traccia che dice qualcosa del suo autore

[45] F. ROMEO, *Memi e libertà di scelta*, in F. RIMOLI, G. M. SALERNO (a cura di), *Conoscenza e potere. Le illusioni della trasparenza*, Carocci, Roma, 2006, p. 261.
[46] A. PUNZI, *Dialogica del diritto*, cit., p. 267.
[47] D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2001, p. 121.

senza però poterlo rappresentare nella sua integralità. […] La persona […] eccede i suoi dati, si annuncia in essi e al contempo se ne ritrae. […] Il dato non è di *proprietà esclusiva* della persona: è un segno lasciato da un soggetto che si è *dato* nel mondo"[48]. "Noi siamo i nostri dati"[49], osserva Stefano Rodotà, che è stato tra i primi ad occuparsi del rapporto tra tutela della privacy[50] e della libertà individuale e nuove tecnologie, già nel lontano 1973, con un suo saggio, *Elaboratori elettronici e controllo sociale*, un manifesto delle libertà individuali nell'epoca della globalizzazione. Il giurista scrive che "senza una forte tutela del *corpo elettronico*, dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo e si rafforzano le spinte verso la costruzione di una società della sorveglianza […]: diventa così evidente che la privacy è uno strumento necessario per salvaguardare la *società della libertà*"[51]. L'espressione "società della sorveglianza" è stata ascritta a David Lyon, che ha analizzato, in maniera approfondita, gli effetti prodotti sul comportamento umano dai nuovi mezzi di controllo sociale, sempre più interconnessi alle tecnologie informatiche. Lyon, ne *La società sorvegliata: tecnologie di controllo della vita quotidiana*, rifiuta ogni giudizio aprioristico sulla sorveglianza, affermando più

[48] A. PUNZI, *Dialogica del diritto*, cit., p. 272.
[49] S. RODOTÀ, *Prefazione*, in D. LYON, *La società sorvegliata*, cit., p. X.
[50] Tappa decisiva nel processo formativo della tutela della privacy nel nostro ordinamento è stata la legge n. 675 del 1996 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali), modellata sulla direttiva comunitaria in materia di trattamento dei dati personali (dir. 95/46/CE), anche se il referente normativo del provvedimento va rintracciato in primis nell'Accordo di Schengen del 1985, che prevedeva la graduale soppressione dei controlli alle frontiere e la promozione della libertà di circolazione delle persone e delle merci e ancora prima nella Convenzione di Strasburgo adottata dal Consiglio d'Europa nel 1981. Attualmente la disciplina sul trattamento dei dati personali è contenuta nel Codice della Privacy adottato nel 2003 che ha coordinato, razionalizzato e innovato la normativa preesistente in materia di dati personali (d.lgs.196/2003). Il testo unico della privacy non ha solo recepito il diritto alla riservatezza nella sua valenza costituzionale, ma ha introdotto un sistema di tutela che difende questo diritto a fronte dei pericoli insiti nei processi di raccolta, elaborazione e circolazione dei dati personali.
[51] S. RODOTÀ, *Intervista su privacy e libertà*, (a cura di P. Conti), Laterza, Roma-Bari, 2005, p. 148.

volte di volerne mettere in evidenza al contempo rischi e benefici. "La sorveglianza", egli dichiara, "è come un giano bifronte", un carattere della postmodernità e da essa è impossibile sfuggire. Rodotà, nella prefazione al saggio dell'autore canadese, sottolinea come "una gabbia elettronica, al posto di quella d'acciaio di weberiana memoria, [venga] implacabilmente costruita intorno a ciascuno di noi e [come sia impossibile liberarsene] con una negazione o una semplice repulsa"[52]. Si viene così a delineare una società dell'integrale trasparenza, che postula l'"uomo di vetro", argomentando che la sorveglianza continua e generalizzata, nonché la cancellazione "d'ogni ragionevole brandello di *privacy*, potrebbero inquietare solo chi ha qualcosa da nascondere. Eppure l''uomo di vetro' è metafora nazista che legittima la pretesa dello Stato di chiedere e ottenere qualsiasi informazione e che implica la classificazione come 'sospetto' e 'cattivo cittadino', come 'nemico dello Stato', di chiunque intenda mantenere spazi d'intimità, esercizio libero di diritti"[53]. Bisogna tuttavia "sottrarre la persona alla 'dittatura dell'algoritmo', emblema di una società della spersonalizzazione, nella quale scompare la persona del decisore, sostituito appunto da procedure automatizzate; e scompare la persona in sé considerata, trasformata in oggetto di poteri incontrollabili"[54].

Si è assistito ad una riconfigurazione della società, in cui "l'uomo non è più soggetto artefice, ma oggetto dell'artificio, insieme funzione e prodotto di un meccanismo da lui stesso messo in movimento ma ormai sfuggito al suo controllo"[55]. L'era digitale potrebbe produrre soltanto maschere, soggetti addomesticati, scattanti di fronte a ogni vibrazione video, in un *media landscape* che ingannevolmente invita alla libertà perché fatto di cartapesta digitale, mentre vera resta la catena della solitudine. Non si deve dimenticare, però, che se è vero che si è sempre più esposti a condizionamenti che possono insidiare la capacità di scegliere liberamente, è vero anche che l'individuo è

[52] S. RODOTÀ, *Prefazione*, in D. LYON, *La società sorvegliata*, cit., p. VIII.
[53] S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 2004, p. 175. Si veda anche ID., *La vita e le regole. Tra diritto e non diritto*, Milano, Feltrinelli, 2006, p. 104.
[54] ID., *Il mondo nella rete. Quali diritti, quali vincoli*, Editori Laterza, Bari, 2014, pp. 37-38.
[55] A. PUNZI, *Dialogica del diritto*, cit., p. 24.

sufficientemente in grado di controllare l'istinto e l'emotività per valutare in modo obiettivo, tra varie alternative, quale sia la scelta migliore[56].

E, allora, per concludere, si azzarda una considerazione sulla tanto ambiziosa domanda: il soggetto digitale è padrone della sua volontà, è ancora libero di scegliere? Non si intende dare una risposta, per dirla con Umberto Eco, "apocalittica" o "integrata"[57], ma appare necessaria una seria riflessione su tale interrogativo e, forse, porsi la domanda risulta più utile che darsi la risposta. Indubbiamente il chiedersi se si può essere liberi porta già con sé il desiderio di libertà, ma la società contemporanea si trova dinanzi a un mutamento di paradigmi che non consente di assumere posizioni definite. Di fatto si è impreparati al

[56] La nozione codicistica di volontà intesa come capacità di volere porta inevitabilmente a compiere alcuni richiami penalistici. Non vi è dubbio che tutti i sistemi evoluti del nostro tempo siano saldamenti imperniati sul cosiddetto principio di colpevolezza, sull'idea, cioè, che la colpevolezza individuale dell'autore costituisca un presupposto indispensabile per l'applicazione della pena. "Alla base dell'idea di colpevolezza c'è la convinzione che l'uomo sia sufficientemente in grado, di regola, di signoreggiare i propri istinti, così da reagire agli stimoli esterni non in modo meccanico, ma utilizzando le proprie facoltà intellettive per scegliere fra diverse possibilità di condotta e quindi orientando le proprie scelte secondo sistemi di valori. L'idea dell'uomo come essere libero e consapevole orienta il principio di colpevolezza, nella sua prospettazione originaria, in cui esso appare strettamente legato al dogma della libertà di volere" (C. FIORE, S. FIORE, *Diritto Penale*, Utet, Torino, 2005, p. 369). La sentenza 364/88 della Corte Cost. ha rappresentato una tappa fondamentale nel percorso di identificazione tra il carattere personale della responsabilità penale e il principio di colpevolezza. Secondo tale pronuncia i padri costituenti, nel disporre all'art. 27 Cost. primo comma che la responsabilità penale debba avere carattere personale, hanno inteso esprimere la necessità che "il fatto sia opera di chi lo ha commesso, non solo da un punto di vista della causazione materiale, ma in quanto prodotto delle scelte di un agente che si trova nelle condizioni di governare i propri impulsi e di orientarli in un modo piuttosto che in un altro" (*ivi*, p. 377). L'art. 85 c.p. prescrive che "nessuno può essere punito per un fatto preveduto dalla legge come reato, se, al momento in cui lo ha commesso, non era imputabile. È imputabile chi ha la capacità d'intendere e di volere". Da tale formula legislativa si desume che la capacità di volere è "la capacità di controllare i propri impulsi e di orientare le proprie determinazioni di volontà alla stregua del significato e della portata del proprio agire nel mondo esterno (*ivi*, p. 399).

[57] Il riferimento è a U. ECO, *Apocalittici e integrati. Comunicazioni di massa e teorie della cultura di massa*, Bompiani, Milano, 1964.

cospetto di scenari che si presentano come qualcosa di costantemente inedito. La maggior parte degli individui ignora gli effetti e le ripercussioni, anche e soprattutto in tema di libertà, che le nuove tecnologie possono provocare. Di certo chi non detiene il potere, "la chiave per controllare, epurare o dirigere ogni unità di informazione e ogni presenza fenomenica sulla rete"[58] non può definirsi libero, l'inconsapevolezza porta a non poter essere liberi di scegliere, ma forse l'uomo può schivare la minaccia dell'organizzazione totale. Esiste la possibilità di una riduzione delle realtà individuali a indifferenziata *massa digitale*, ma forse la salvezza è nella direzione del pericolo[59]: solo affrontando il rischio, al contempo con prudenza e coraggio, solo assecondando con cautela il vortice del progresso si potrà tentare di conoscerne i risvolti e probabilmente uscirne indenni. Affermare l'esistenza della libertà di scelta nell'era digitale appare azzardato quanto escluderla del tutto. Se è vero, come sostiene Walter Benjamin, che "al pensiero non appartiene solo il movimento delle idee, ma anche il loro arresto"[60], conferendo problematicità al progresso che a volte genera la propria negazione, perché definito dalla distruzione del passato e dalla violenta antitesi tra natura e artificio, è vero anche che l'uomo può e deve osare attraversando inesplorati percorsi e scoprendo l'ignoto con la consueta curiosità che lo contraddistingue. "È giunta l'ora, dunque, che lo stesso consumatore postmoderno, ormai sufficientemente alfabetizzato in ordine ai linguaggi e strategie della società dello spettacolo permanente, rinunci a farsi scudo del suo preteso stato di minorità e, dove possibile, si assuma appieno le sue responsabilità di attore del proprio tempo"[61].

"Fatti non foste a viver come bruti, ma per seguir virtute e conoscenza": l'esortazione dantesca può ancora oggi rappresentare l'invito per l'uomo a cercare, senza smarrire il senso di responsabilità,

[58] M. HEIM, *Ontologia erotica del ciberspazio*, in M. BENEDIKT (a cura di), *Cyberspace: primi passi nella realtà virtuale*, Muzzio, Padova, 1993, p. 84.
[59] Cfr. M. HEIDEGGER, *La questione della tecnica*, in Id., *Saggi e discorsi*, a cura di G. VATTIMO, Mursia, Milano,1976, p. 22.
[60] W. BENJAMIN, *Angelus Novus*, Torino, Einaudi, 1995, p. 85.
[61] A. PUNZI, *Dialogica del diritto*, cit., p. 312.

nuove strade e spostare di continuo i traguardi di quel suo inarrestabile e metaforico viaggio verso ciò che è ancora sconosciuto.

Rassegna giuridica

Provvedimenti del Garante

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Parere all'AGID su due schemi di regolamento recanti, rispettivamente, le modalità attuative per la realizzazione dello SPID e le relative regole tecniche - 4 giugno 2015

in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/print/4257475

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

Vista la richiesta di parere dell'Agenzia per l'Italia digitale;

Visto l'articolo 154, comma 4, del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, di seguito Codice);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Antonello Soro;

PREMESSO

L'Agenzia per l'Italia digitale (di seguito AGID) ha richiesto il parere del Garante su due schemi di regolamento recanti, rispettivamente, le modalità attuative per la realizzazione dello SPID e le relative regole tecniche.

I regolamenti sono adottati ai sensi dell'articolo 4, comma 2, del decreto del Presidente del Consiglio dei ministri 24 ottobre 2014 (di seguito dPCM) recante la definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema da parte delle pubbliche amministrazioni e delle imprese, sul cui schema il Garante ha reso parere in data 19 giugno 2014.

L'articolo 4 del dPCM, infatti, ai commi 2, 3 e 4, prevede che l'AGID adotti regolamenti per definire, appunto, le regole tecniche e le modalità attuative per la realizzazione dello SPID, le modalità di accreditamento dei soggetti SPID, nonché le procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale. Con tali regolamenti devono essere disciplinati anche altri profili, richiamati in altri articoli del decreto.

Anche gli schemi degli altri provvedimenti sono stati trasmessi al Garante; in data 23 aprile scorso, l'Autorità ha reso, infatti, parere sullo schema di regolamento concernente l'accreditamento dei gestori di identità digitale, e su quello recante le procedure necessarie a consentire ai predetti gestori, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale.

Il presente parere – per evidenti ragioni di affinità di materia – si riferisce a entrambi i regolamenti i cui schemi sono stati trasmessi.

RILEVATO

1. Il sistema SPID.

Occorre premettere che lo SPID consente agli "utenti" (persone fisiche o giuridiche che utilizzano i servizi erogati in rete) di avvalersi di specifici soggetti, i "gestori dell'identità digitale", per consentire ai "fornitori di servizi" l'immediata verifica della propria identità e di eventuali "attributi qualificati" che li riguardano (art. 2 dPCM).

I soggetti pubblici o privati che partecipano allo SPID sono: i gestori dell'identità digitale ("le persone giuridiche accreditate allo SPID che, in qualità di gestori di servizio pubblico, previa identificazione certa dell'utente, assegnano, rendono disponibili e gestiscono gli attributi utilizzati dal medesimo utente al fine della sua identificazione informatica. Essi inoltre, forniscono i servizi necessari a gestire l'attribuzione dell'identità digitale degli utenti, la distribuzione e l'interoperabilità delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti"); i "gestori degli attributi qualificati"; i fornitori di servizi (definiti quali fornitori dei servizi della società dell'informazione, ex art. 2, comma 1, lett. a), d. lg. n. 70/2003 o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili al pubblico); l'Agenzia per l'Italia digitale e gli utenti. Tali soggetti, eccettuati gli utenti, costituiscono un sistema aperto e cooperante che consente loro di comunicare utilizzando meccanismi di interazione, standard tecnologici e protocolli indicati nel decreto e dettagliati nelle regole tecniche definite dall'AGID con proprio regolamento (art. 3 dPCM).

Per "identità digitale" si intende la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale (art. 1, comma 1, lett. o)). Premesso che per "attributi" si intendono le informazioni o la qualità di un utente utilizzate per rappresentare la sua identità, il suo stato, la sua forma giuridica o altre caratteristiche peculiari, lo schema distingue fra: "attributi identificativi" (nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonché il codice fiscale e gli estremi del documento d'identità utilizzato ai fini dell'identificazione); "attributi non identificativi" (il numero di telefonia mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonché eventuali altri attributi individuati dall'AGID); "attributi qualificati" (le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati) (art. 1, comma 1, lett. a), b), c) e d)).

Le identità digitali rilasciate all'utente contengono obbligatoriamente il "codice identificativo" e gli attributi identificativi e possono contenere gli attributi non identificativi, gli attributi qualificati e ulteriori attributi registrati su richiesta dell'utente nell'ambito delle categorie individuate dall'AGID tramite i regolamenti di cui all'articolo 4.

2. Il regolamento recante le modalità attuative.

Il regolamento si compone di quattro capi, recanti nel complesso 32 articoli, e cinque appendici.

Esso disciplina le modalità di rilascio dell'identità digitale e delle relative credenziali previa identificazione (a vista, a vista da remoto, tramite documenti digitali di identità, tramite altre identità SPID, tramite firma elettronica qualificata o firma digitale) e verifica dell'identità dichiarata dal richiedente diversificando, laddove necessario, i requisiti nel caso di persona fisica o giuridica.

È regolato il ciclo di vita dell'identità digitale (rilascio, gestione degli attributi, sospensione e revoca) e delle credenziali (creazione, consegna, attivazione delle credenziali o dei mezzi usati per la loro produzione, conservazione, sospensione e revoca delle credenziali o dei mezzi usati per la loro produzione, rinnovo e sostituzione delle credenziali o mezzi usati per la loro produzione).

Inoltre è definito lo scenario di utilizzo di SPID che comprende: le interazioni fra i diversi attori, l'uso degli attributi SPID, la gestione delle sessioni di autenticazione differenziata per livelli SPID, gli elementi utili al sistema nel suo complesso (Servizio di discovery, Registro SPID, Directory delle identità SPID), la conservazione delle informazioni delle richieste di autenticazione al proprio gestore di identità da parte degli utenti.

Infine è disciplinato il monitoraggio di AGiD sul sistema SPID allo scopo di valutare e garantire usabilità, accessibilità e corretto utilizzo degli elementi identificativi SPID.

Le Appendici recano disposizioni in materia di: A) criteri per l'attribuzione dei livelli di sicurezza dei servizi (descrive, a titolo

esemplificativo, una metodologia per il fornitore dei servizi per determinare i livelli di sicurezza dei servizi); B) minacce associate alla gestione del ciclo di vita delle identità digitali (illustra le possibili minacce in riferimento alle varie fasi del ciclo di vita delle identità digitali e alle varie tipologie di token e alcune strategie di mitigazione); C) tipi di token e loro tassonomia (riporta i principali tipi di token utilizzabili per l'autenticazione informatica); D) usabilità e accessibilità (individua un percorso comune per l'esperienza utente); E) disciplina sull'utilizzo degli elementi grafici identificativi dello SPID (stabilisce elementi quali il logo, i colori e i caratteri tipografici identificativi del sistema SPID).

3. Il regolamento recante le regole tecniche.

Il regolamento disciplina gli scenari di interazione, le specifiche delle interfacce, i contenuti e i formati dei messaggi di autenticazione e autorizzazione (asserzioni) scambiati tra i diversi attori del sistema - gestore dell'identità digitale, fornitore di servizi, gestore di attributi qualificati e utente che richiede l'accesso a un servizio – secondo il protocollo SAML (Security Assertion Markup Language – versione 2).

Le interazioni avvengono su canale sicuro e i diversi messaggi sono firmati digitalmente dai diversi attori. Sono regolamentati, inoltre, il contenuto, il funzionamento e l'accesso:

a) al Servizio di discovery: che consente a un fornitore di servizi di individuare quale gestore dell'identità digitali fornisce l'identità SPID all'utente che richiede un servizio;

b) al Registro SPID: la base dati che contiene le informazioni sui soggetti partecipanti allo SPID (gestori dell'identità digitale, gestori degli attributi qualificati e fornitori di servizi) quali, a esempio, l'identificatore SAML dell'entità, la denominazione del soggetto a cui afferisce l'entità della federazione, il tipo di entità, l'URL del servizio di reperimento metadati e l'elenco di attributi qualificati certificabili;

c) alla Directory delle identità SPID: la base dati che contiene le associazioni tra gli identificativi delle identità degli utenti SPID e il relativo gestore di identità.

Infine sono indicate, a titolo esemplificativo e non esaustivo, le informazioni che i gestori dell'identità digitale dovranno registrare in un apposito Registro delle transazioni per la tracciabilità delle richieste di autenticazione e le modalità con cui le stesse dovranno essere conservate.

RITENUTO

4. La complessità e le criticità del Sistema.

Il Garante riconnette particolare importanza alla materia in esame, in ragione della delicatezza dei trattamenti di dati personali previsti e dei profili di sicurezza informatica implicati.

Il sistema SPID è infatti prefigurato quale servizio infrastrutturale di cui fruiranno milioni di cittadini, le imprese e l'intera pubblica amministrazione, con l'obiettivo di una forte riduzione dei costi di gestione degli utenti o consumatori online da parte dei soggetti pubblici e privati operanti come fornitori di servizi in rete, favorendo nel contempo l'espansione del commercio elettronico e l'innovazione digitale della pubblica amministrazione.

È pertanto evidente come il costituendo SPID si avvii a divenire una vera e propria infrastruttura critica, la cui disponibilità e il cui corretto esercizio saranno precondizione per il funzionamento di larga parte dei servizi informatici online, sia di tipo business-to-consumer che business-to-business, e per l'efficiente fruizione di servizi e informazioni pubbliche da parte degli utenti.

Alla luce di queste considerazioni preliminari, appare evidente come una non adeguata valutazione dei profili di sicurezza possa esporre l'intera infrastruttura a una diversificata casistica di rischi informatici, derivanti da furto, uso abusivo, o alterazione dell'identità degli interessati (con tecniche di phishing, diffusione di malware e di agenti software di controllo remoto, contraffazione digitale di siti e servizi

online), rispetto ai quali vi è ancora in Italia una carente consapevolezza, con conseguente limitatezza degli interventi correttivi, anche nei settori delicati delle diverse realtà economiche, produttive, istituzionali.

Ad accrescere il rischio potenziale derivante da azioni fraudolente è la caratteristica connaturata di SPID quale sistema d'elezione per l'accesso ai servizi online delle pubbliche amministrazioni e delle imprese, la cui compromissione a seguito di attacco informatico, anche solo nelle forme non direttamente distruttive del denial of service (DoS), avrebbe ripercussioni sulla fruibilità di servizi e di dati, anche personali, su scala nazionale e non solo nell'ambito della pubblica amministrazione.

Occorre quindi applicare particolare cura agli aspetti di sicurezza, poiché solo la presenza di adeguati meccanismi di garanzia può consentire l'acquisizione e il mantenimento della fiducia degli utenti nel nuovo sistema di identità digitale, mentre basterebbero pochi incidenti, anche di limitato impatto, per minare alla base la possibilità di fare del sistema SPID uno dei volani dell'innovazione digitale nel nostro Paese.

Nell'esprimere il presente parere il Garante tiene quindi in alta considerazione, nell'ambito dei profili di propria competenza istituzionale, gli aspetti di sicurezza dei trattamenti nello SPID, evidenziando come tali aspetti non appaiano esser stati oggetto di specifiche valutazioni preventive nell'ambito di un'analisi dei rischi di cui sia traccia nei regolamenti in esame, al di là di generiche e schematiche indicazioni relative ai livelli di sicurezza corrispondenti ai differenti metodi di autenticazione informatica previsti.

Tale impressione è probabilmente favorita dall'assenza di una relazione illustrativa dei regolamenti sottoposti a parere, che vengono quindi qui valutati sulla scorta del loro letterale contenuto e sulla base dei chiarimenti forniti direttamente dai rappresentanti dell'Agenzia nel corso dei diversi incontri svolti, nel corso della fase istruttoria, con il personale dell'Autorità impegnato nella trattazione del procedimento.

In relazione agli aspetti generali di sicurezza del sistema, si osserva come SPID sia basato, nella sua componente tecnologica, sui protocolli SAML 2.0 (Security Assertion Markup Language) per l'autenticazione e l'interscambio di dati di sicurezza. I protocolli SAML sono definiti e promossi come standard aperto dal consorzio OASIS (Organization for the Advancement of Structured Information Standards), e trattano con la dovuta accuratezza gli aspetti di sicurezza informatica, che andrebbero quindi maggiormente esplicitati in entrambi i regolamenti, menzionando quanto meno le "Security considerations" di SAML 2.0 nonché l'Errata del 2012 (che comprende indicazioni sulla c.d. RelayState sanitization per mitigare i rischi di Cross Site Scripting (XSS) cui può essere esposto un Service Provider).

Relativamente al rispetto dei principi di necessità e proporzionalità del trattamento, non sono evidenziate le cautele adottate affinché, nei casi in cui per accedere a un servizio online sia sufficiente provare il possesso di alcuni attributi (ad es. la maggiore età), non sia necessario mostrare in chiaro la propria identità o propri attributi.

È necessario, per assicurare il rispetto di tali principi, adottare in SPID le opportune modalità tecniche contemplate dallo standard SAML 2.0 come i "Transient Pseudonym Identifiers" ivi previsti, mentre questa possibilità sembra al momento esclusa.

Nell'ambito di una complessiva analisi dei rischi, andrebbe valutata l'adozione di accorgimenti a protezione della fase di transito delle asserzioni (sia di autenticazione che di attributo) all'interno del browser, nonché quella di misure di protezione contro il rischio di replay attacks incombente sugli Identity Provider.

Riguardo all'identificativo utente, su cui vengono formulate specifiche osservazioni nel seguito in riferimento ad alcuni articoli del Regolamento sulle modalità attuative, è opportuno che il suo formato non sia necessariamente quello di indirizzo email, per due ordini di motivi. In primo luogo, non è richiesto a livello di protocolli SAML che ciò avvenga, ben potendosi utilizzare, a tale scopo, il codice identificativo, di cui all'articolo 1, comma 1 lettera g) del dPCM. Gli utenti potrebbero utilizzare direttamente tale codice identificativo,

assegnato a ciascuno dal proprio gestore dell'identità digitale e contenente la codifica univoca dello stesso gestore, utile in fase di autenticazione per individuare direttamente il gestore competente a fornire le asserzioni.

Secondariamente, appare macchinosa la procedura relativa alle richieste di identità digitali ulteriori, laddove l'assegnazione forzosa di un indirizzo email aggiuntivo potrebbe essere evitata, ammettendo l'uso di uno stesso indirizzo per più identità digitali, e lasciando alla componente di discovery il compito di individuare la lista di gestori dell'identità digitale in grado di fornire asserzioni relativamente a un determinato utente.

Infine, l'introduzione in un'architettura federata e distribuita come quella SPID di un componente architetturale fortemente centralizzato come quello necessario per realizzare la funzionalità di discovery comporta la costituzione di un single point of failure che, oltre a gravare con ogni probabilità sulle prestazioni del sistema, diventa pericolosamente esposto ad attacchi che, nel caso di Distributed Denial of Service particolarmente incisivi, potrebbero avere come conseguenza il blocco complessivo di SPID, risultando quindi oltremodo paganti per creare disservizi e compromettere la fiducia nella nuova infrastruttura.

Relativamente all'uso degli attributi anche qualificati, non è chiara la gestione delle asserzioni in termini di retention da parte dei fornitori di servizio, che potrebbero conservarle indefinitamente e senza adeguata protezione, e in maniera eccedente (dal punto di vista temporale) rispetto all'erogazione dei servizi.

5. L'articolato recante le modalità attuative e il documento sulle regole tecniche.

Ferme restando le preoccupazioni espresse al punto 4 in ordine alle evidenziate criticità del sistema, l'Autorità esamina, ora, gli schemi di regolamento trasmessi.

In ragione della complessità e delicatezza della materia, lo schema di regolamento è stato elaborato dall'AGID all'esito di numerose

riunioni e interlocuzioni avute con l'Ufficio del Garante il quale ha formulato rilievi e ha fornito indicazioni volte a perfezionare il testo e a renderlo pienamente conforme alla disciplina in materia di protezione dei dati personali.

Ciononostante, l'Autorità deve responsabilmente rilevare che molte delle disposizioni del provvedimento non sono chiaramente definite o elaborate, con conseguenti ambiguità che potrebbero pregiudicare l'attuazione uniforme del regolamento stesso da parte dei soggetti che partecipano allo SPID. Lo schema, perciò, deve essere fortemente migliorato, anche dal punto di vista formale, e probabilmente anche integrato in relazione ad aspetti che non sono, allo stato, trattati e in assenza dei quali il sistema non potrebbe entrare a regime. Si fa rifermento, ad esempio, alla procedura di accreditamento dei gestori di attributi qualificati, alle modalità per consentire agli utenti la rimozione dei dati contenuti nell'identità digitale, nonché agli schemi di convenzione tra l'Agenzia e i fornitori di servizi (v. artt. 4, comma 1, lett. c), 8, comma 2, 13, comma 2, dPCM).

Più in particolare, si richiama l'attenzione dell'Amministrazione sull'opportunità di verificare puntualmente la congruenza delle disposizioni del regolamento con quelle del dPCM (salvo, ovviamente, eventuali precisazioni di dettaglio), a cominciare dall'utilizzo delle definizioni in esso contenute (art. 1, dPCM), cui lo schema, peraltro, deve fare formale rinvio con una norma ad hoc. Va inoltre evidenziata l'opportunità di non ripetere nel regolamento – a titolo meramente ricognitivo – disposizioni già contenute nel dPCM. È importante, pure, che sia verificata la puntuale coerenza del regolamento sulle modalità attuative con le disposizioni contenute nelle appendici allegate e nelle relative regole tecniche, ed assicurato il coordinamento del medesimo con i due regolamenti sui cui schemi il Garante ha già reso parere (in tema di accreditamento dei gestori dell'identità digitale e di particolari modalità per il rilascio dell'identità; v. in premessa).

Al riguardo, ad esempio, è necessario conformare il comma 1 dell'articolo 2 dello schema di regolamento al dettato dell'articolo 3, comma 1, del dPCM e alle definizioni dei "soggetti partecipanti allo

SPID" contenute nel medesimo dPCM. In particolare, quest'ultimo annovera fra i soggetti in questione l' "utente" e non il "richiedente" (ciò non toglie che l'espressione "richiedente" possa essere utilizzata nel regolamento per indicare la persona che richiede il rilascio dell'identità digitale, come correttamente previsto all'articolo 5). Come pure – e sempre a solo titolo esemplificativo – nell'articolo 19 e ovunque ricorra si deve fare riferimento all' "utente" invece che al "titolare dell'identità digitale".

Si raccomanda inoltre di utilizzare – per quanto possibile – una terminologia coerente con gli istituti giuridici vigenti e conforme alla normativa di settore e di ricorrere preferibilmente ad espressioni chiare e semplici (da questo punto di vista, ad esempio, sono sicuramente da chiarire le locuzioni "fonti autoritative istituzionali", in art. 12, e "self caring" in art. 19; si segnala, poi, all'art. 19, ultimo comma, un evidente refuso, posto che l'ANPR non è una pubblica amministrazione, ma una banca dati).

Ciò premesso, il presente parere elaborerà ulteriormente i temi già affrontati in via collaborativa con l'AGID, al fine di migliorare le attuali disposizioni della proposta, in termini sia di chiarezza che di coerenza normativa, ma esclusivamente in relazione agli aspetti di protezione e di sicurezza dei dati personali, nei termini di seguito descritti.

5.1. Si apprezza la scelta di inserire già nell'articolo 2 del regolamento una disposizione di richiamo delle caratteristiche del sistema e dei trattamenti in senso conforme alle garanzie previste in materia di protezione dei dati personali. La norma va però perfezionata, sostituendola con la seguente: "Il Sistema SPID si conforma al principio di necessità nel trattamento dei dati di cui all'articolo 3 del decreto legislativo 30 giugno 2003, n. 196, in base al quale i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. I trattamenti di dati personali in applicazione del presente regolamento sono effettuati esclusivamente per le finalità previste dall'articolo 64 del CAD e dall'articolo 2, comma 2, del DPCM 24 ottobre 2014 e con

le modalità individuate dal presente regolamento, nel rispetto delle garanzie previste dal medesimo decreto legislativo n. 196 del 2003.".

5.2. Al medesimo articolo 2, deve essere integrata la descrizione dei livelli di sicurezza delle identità digitali SPID al fine di garantire una maggiore coerenza della disposizione con quanto previsto all'art. 8 del Regolamento (UE) n. 910/2014 del 23 luglio 2014, in materia di livelli di garanzia dei mezzi di identificazione elettronica. In particolare, la descrizione dei livelli di sicurezza deve tenere in adeguata considerazione l'affidabilità e la qualità delle specifiche tecniche, norme e procedure che caratterizzano i diversi sistemi di identificazione elettronica predisposti dai gestori dell'identità digitale, volte a ridurre o impedire il rischio di uso abusivo o alterazione dell'identità. Al fine di eliminare ogni ambiguità del testo, occorre inoltre specificare l'ambito di riferimento del rischio menzionato nel medesimo articolo per descrivere i differenti livelli di sicurezza delle identità digitali. Ciò, al fine di mantenere un'opportuna distinzione tra la valutazione, in capo ai gestori dell'identità digitale, del livello di affidabilità e sicurezza dei sistemi di identificazione elettronica predisposti, e, quella, in capo ai fornitori di servizi, dell'impatto per gli utenti interessati di un utilizzo improprio delle loro identità SPID in relazione all'accesso a differenti tipologie di servizi elettronici offerti.

5.3. Deve essere perfezionato il richiamo, contenuto in più punti dello schema, ad alcuni obblighi previsti dal Codice per i gestori dell'identità digitale (informativa all'interessato e consenso al trattamento dei dati personali), tenuto conto che per i trattamenti di dati personali necessari alla gestione delle identità digitali nel sistema SPID effettuati dai gestori delle identità digitali, dai fornitori di servizi e dai gestori degli attributi qualificati non è necessario acquisire il consenso dell'interessato (artt. 18, comma 4, e 24, comma 1, lett. a) e b), del Codice). L'osservazione può essere recepita sopprimendo l'ultimo comma dell'articolo 5 e, al terzo comma, lett. a), dell'articolo 6, le seguenti parole: "e ottiene esplicito assenso".

Analoghe considerazioni valgono in relazione agli articoli 27, commi 2 e 3, e 28, comma 3 (per i quali si rinvia ai pertinenti punti del parere).

Oltre a ciò, è importante che gli utenti (cioè – si ricorda – le persone cui è stata attribuita, a richiesta, un'identità digitale), siano messi in grado di comprendere appieno le potenzialità e quindi anche i rischi di tale infrastruttura. Anche dal punto di vista della sicurezza, il sistema SPID potrà dirsi pienamente funzionante solo con la collaborazione degli utenti del servizio, che dovranno rispettare scrupolosamente alcune regole e, a tal fine, acquisire una piena consapevolezza sulle corrette modalità di utilizzo del sistema.

Da questo punto di vista, si ritiene pertanto necessario integrare l'articolo 6 dello schema prevedendo che i richiedenti il rilascio dell'identità digitale siano informati, più in generale rispetto all'informativa "sulla privacy", in merito alle finalità e all'ambito di utilizzo dell'identità digitale ed ai connessi rischi.

A titolo di collaborazione, si suggeriscono di seguito alcuni elementi di cui gli utenti dovrebbero essere informati, con modalità semplici e chiare: l'ambito di utilizzo di identità digitali SPID e, in particolare, i relativi effetti giuridici nelle transazioni elettroniche; come devono essere gestite le credenziali di accesso o i dispositivi di autenticazione (es. indicazioni per la corretta conservazione, rischi derivanti dall'eventuale condivisione di credenziali e associati al loro eventuale furto o smarrimento); quali possono essere i segnali che indicano che un'identità digitale è stata violata o che sono state usate impropriamente le credenziali; i rischi associati ad un furto di identità e le contromisure da adottare; quali sono i "dati minimi" e sufficienti per l'erogazione di un servizio on line e in quali casi il fornitore del servizio può chiedere ulteriori dati all'utente; le specifiche modalità con cui l'utente può modificare, aggiornare o cancellare i propri dati personali nell'ambito dello SPID o con cui chiedere la sospensione o la revoca della propria identità digitale.

Analoghe considerazioni vanno formulate relativamente all'articolo 16, ultimo comma, in cui si fa riferimento alle informazioni che il gestore dell'identità digitale deve fornire all'utente all'atto della

consegna delle credenziali, coordinando tale disposizione con quella di cui al predetto articolo 6.

5.4. L'articolo 8 – che disciplina l'identificazione del richiedente l'identità digitale a vista da remoto – deve essere perfezionato in relazione agli obblighi previsti in materia di protezione dei dati personali.

Al primo comma, si prevede che tale identificazione avvenga "nel rispetto delle misure prescritte dal Garante per la protezione dei dati personali.". Il Garante non ha specifica competenza in materia di riprese audio-video, se non per i profili generali riguardanti la protezione dei dati personali; si suggerisce, pertanto, di sostituire il periodo sopra riportato con il seguente: "nel rispetto del decreto legislativo 30 giugno 2003, n. 196".

Al settimo e all'ottavo comma, lett. a), si prevede che prima di iniziare la registrazione l'operatore chieda l' "assenso" alla registrazione audio video e il "consenso" alla videoregistrazione.

Al riguardo, al di là dell'utilizzo improprio della locuzione "assenso" in luogo di consenso, si osserva quanto segue.

Premesso che il consenso al trattamento dei dati personali, per essere valido deve essere liberamente espresso, se il gestore dell'identità digitale fornisce solo l'identificazione a vista da remoto come modalità per la verifica dell'identità del richiedente, ciò deve essere messo in specifica evidenza nelle condizioni e termini del contratto; una volta firmato il contratto il trattamento dovrebbe essere considerato necessario per la sua esecuzione e quindi non richiedere il consenso ai sensi dell'articolo 24, comma 1, lett. b), del Codice.

Se invece l'identificazione a vista da remoto è solo una delle modalità predisposte dal gestore per la verifica dell'identità del richiedente, allora dovrebbe essere richiesto un apposito consenso al trattamento dei dati personali contenuti nelle riprese audio/video, possibilmente specificando tale aspetto nell'informativa da rendere all'interessato ai sensi dell'articolo 13 del Codice.

L'articolo deve essere perciò perfezionato tenendo conto delle predette osservazioni.

Al penultimo comma, poi, prevede che la "sessione audio/video deve essere condotta seguendo una procedura scritta certificata dal gestore"; occorre individuare i parametri tecnici e informatici di tale certificazione o, in alternativa, è necessario sostituire il termine "certificata" con "formalizzata".

Inoltre per evitare attacchi di phishing perpetrati attraverso sistemi video o audio (Voice Phishing o Vishing) occorre prevedere opportune misure quali, a esempio, un sistema di mutua autenticazione che consenta di garantire l'identificazione certa, oltre che dell'utente, anche del gestore dell'identità digitale.

La procedura prevista appare farraginosa e non usabile nel caso di dispositivi mobili, a meno di contemplare l'uso simultaneo di più dispositivi da parte del richiedente. Si garantirebbe lo stesso livello di sicurezza prevedendo una procedura di challenge in cui viene chiesto al soggetto richiedente l'inserimento di un numero pseudocasuale inviatogli con messaggio SMS.

Deve essere poi assicurata, con riguardo all'identificazione a vista da remoto in caso di rilascio di credenziali di livello 3, la coerenza con la prescrizione della norma tecnica ISO 29115 relativa al livello di sicurezza LoA4, che prevede la necessità di identificazione di persona.

5.5. All'articolo 9 (Identificazione informatica tramite documenti digitali di identità) va sciolta l'ambiguità dell'ultimo periodo, chiarendo se il gestore è tenuto a verificare la correttezza del processo di identificazione già espletato "a monte" oppure si intenda introdurre una sorta di "presunzione" di correttezza del medesimo processo.

5.6. All'articolo 12, terzo comma, si prevede che "nelle more del completamento" dell'ANPR, i gestori dell'identità e degli attributi, per finalità di verifica dell'esattezza dei dati personali del richiedente l'identità digitale, possano verificare il codice fiscale e i dati anagrafici presso l'Agenzia delle entrate.

La disposizione deve essere coordinata con la normativa in materia di ANPR, tenendo conto dei servizi allo stato forniti attraverso la predetta anagrafe cui, evidentemente, il presente regolamento non potrebbe apportare innovazioni "a regime" (cfr. art. 38, comma 6, d.l.

31 maggio 2010, n. 78 convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122; dPCM 23 agosto 2013, n. 109 e dPCM 10 novembre 2014, n. 194, in particolare, art. 1, comma, 2 e all. A e D).

Sempre all'articolo 12, nella prima tabella (seconda riga), dove si individuano i requisiti della verifica di identità rispetto ai livelli di sicurezza 2 e 3, è riportata la seguente frase: "con specifico riferimento al furto d'identità: deve essere prevista la consultazione dell'Archivio centrale informatizzato di cui al decreto legislativo n. 141 del 2010".

Premesso che la disposizione non chiarisce dove dovrebbe essere prevista tale consultazione (e con riferimento a quali soggetti), si rileva che l'archivio cui si fa cenno, istituito nell'ambito del Ministero dell'economia e delle finanze, riguarda la materia della prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo e dei pagamenti dilazionati o differiti, con specifico riferimento al furto di identità (art. 30-quater, d. lg. n. 141/2010 e successive modificazioni; d.m. 19 maggio 2014, n. 95), materia affatto diversa da quella regolamentata nel presente provvedimento. Pertanto, è necessario espungere dalla tabella ogni riferimento al predetto archivio.

5.7. L'articolo 13 (Conservazione e registrazione dei documenti), all'ultimo comma, stabilisce che tutta la documentazione inerente alla creazione e al rilascio di una identità digitale deve essere conservata ai sensi dell'articolo 7, commi 8 e 9 del DPCM.

Al riguardo, posto che il citato comma 9 non fa altro che richiedere il rispetto della normativa in materia di protezione dei dati personali e considerato che i predetti documenti sono particolarmente rilevanti ai fini dell'affidabilità del processo di rilascio delle identità digitali, si richiama l'attenzione dell'AGID sull'opportunità di integrare l'articolo 13 dello schema con l'individuazione in concreto di specifici obiettivi di sicurezza che i gestori dovranno assicurare per garantire una conservazione adeguata e protetta della documentazione e delle informazioni acquisite, nonché modalità di accesso selettivo ai dati personali, tenuto conto anche della durata ventennale del periodo di conservazione previsto dal dPCM (art. 31 del Codice).

Analoga integrazione deve essere prevista in relazione all'articolo 8, ultimo comma, (dove si fa riferimento ai "dati di registrazione" acquisiti nella procedura di identificazione da remoto, costituti da file audio-video, immagini e metadati strutturati in formato elettronico), coordinando le due disposizioni.

5.8. L'articolo 14, primo comma, nel descrivere il contenuto dell'identità digitale, vi include anche l' "identificativo utente" (lett. d)), insieme agli attributi identificativi e agli attributi secondari dell'utente, nonché al codice identificativo dell'identità digitale. Tale "identificativo utente" viene poi definito quale attributo secondario corrispondente all'indirizzo di posta elettronica comunicato dal richiedente al momento della richiesta dell'identità.

L'articolo 14 va modificato espungendovi ogni riferimento a tale identificativo, non solo perché esso non è previsto dal dPCM quale elemento costitutivo obbligatorio dell'identità digitale (art. 5), ma anche perché questo dato risulta eccedente rispetto alle finalità perseguite con il rilascio dell'identità digitale e all'esigenza di riferibilità certa dell'identità digitale all'utente. Resta fermo che l'indirizzo di posta elettronica fornito dall'interessato quale attributo secondario potrà (e dovrà) essere utilizzato dal gestore per la sua precipua finalità (comunicazione di informazioni: art. 1, comma 1, lett. d), dPCM).

5.9. L'articolo 15 sulla creazione delle credenziali prevede che per il Livello 1 SPID le password non vengano generate in modo completamente casuale; tale previsione appare tecnicamente controproducente perché, fissati l'alfabeto ammesso e le regole per la composizione, la generazione delle password dovrebbe essere la più casuale possibile, per evitare attacchi dictionary based.

Andrebbe inoltre vietata l'inclusione nelle password di informazioni non segrete riconducibili al titolare, in luogo della raccomandazione sul divieto d'uso di "formati comuni".

Nello stesso articolo, in relazione alle modalità di generazione della OTP (one-time password), andrebbe contemplata la codifica dell'OTP nel numero (variabile) del chiamante, senza ricorso al servizio di

SMS; inoltre, la connettività in rete prevista per l'utilizzo di "applicazioni mobile per smartphone e tablet" appare non strettamente necessaria per la fase di generazione della OTP se si mettono a disposizione strumenti PRNG (pseudo-random numbers generator) in forma di applicazione stand-alone, che non richiedono quindi la connessione di rete per generare la password temporanea, al pari di dispositivi dedicati.

5.10. All'articolo 16, secondo comma, lett. b), deve essere soppressa la parola "minime" in quanto, com'è noto, l'obbligo gravante in materia di sicurezza su ogni titolare del trattamento è volto a ridurre al minimo i rischi di distruzione dei dati degli interessati o di accessi abusivi ai sistemi, mediante misure "idonee" a tale scopo (art. 31 del Codice), e non si esaurisce, pertanto, nell'adozione delle misure minime di cui all'allegato B del Codice.

5.11. L'articolo 18 (Segnalazioni sull'utilizzo delle credenziali) deve essere perfezionato, precisando che, le notifiche devono essere attivate in assenza di richiesta specifica contraria (attivazione per default) e non soltanto a seguito della esplicita richiesta di attivazione da parte dell'utente. Vanno altresì specificate le informazioni che il gestore dell'identità digitale invia all'utente, indicate nel testo dell'articolo con il generico termine "estremi". Le notifiche andrebbero estese anche al caso di creazione di nuova identità digitale a partire da una esistente disciplinato nell'Art. 10.

5.12. In relazione a quanto previsto all'articolo 19 (Gestione degli attributi), poiché gli aggiornamenti degli attributi identificativi sono resi possibili all'utente tramite un'area web del gestore dell'identità digitale, dedicata a tale scopo, accessibile mediante credenziali almeno di livello 2, occorre integrare la disposizione specificando le modalità con cui un utente con credenziali di livello 1 possa aggiornare i propri attributi.

5.13. In relazione a quanto previsto agli articoli 22 (Conservazione delle credenziali) e 23 (Sospensione e revoca delle credenziali), si richiama l'attenzione dell'AGID sull'opportunità di dettagliare, rispettivamente, le prescrizioni per la conservazione delle credenziali,

in particolare per quelle di livello 2 e 3, e le modalità con cui l'utente può richiederne la sospensione o la revoca.

5.14. All'articolo 25, al fine di chiarire i diversi ruoli dei soggetti partecipanti allo SPID durante il processo di autenticazione, al primo comma, dopo le parole: "dimostra la propria identità" devono essere inserite le seguenti: "al gestore dell'identità digitale".

Inoltre, il terzo comma va perfezionato chiarendo che la prima fase di interazione fra utenti e fornitori di servizi non deve comportare la raccolta di dati personali diversi da quelli strettamente necessari all'interazione tramite protocolli di rete.

Va inoltre perfezionato il punto 3) del terzo comma, specificando che – come sembra – l'asserzione di autenticazione SAML non deve attestare attributi quando non necessari alla fruizione del servizio, ma può, invece, attestare esclusivamente l'esito della verifica (producendo cioè una risposta di tipo "booleano") effettuata dal gestore dell'identità, che può eventualmente riguardare anche i soli attributi non identificativi dell'interessato. In ogni caso, il gestore dell'identità deve mettere a conoscenza l'utente degli attributi richiesti dal fornitore del servizio (cfr. punto 5.15. in relazione ad art. 27).

Devono, poi, essere previste regole stringenti di segregation of duty, nel caso in cui uno stesso soggetto sia, allo stesso tempo gestore dell'identità digitale e fornitore di servizi. In tal caso, devono essere mantenuti separati i log di tracciatura delle transazioni così come le banche dati relative alla gestione delle identità digitali, in capo al gestore, dalle banche dati relative ai servizi erogati. Tale vincolo di separazione deve essere applicato anche nei confronti degli accessi degli operatori di help desk e nella gestione di cruscotti di self caring che vanno mantenuti separati (art. 19).

Inoltre, per aumentare il livello di sicurezza dell'intero processo, evitando in particolare possibili attacchi di tipo phishing e man-in-the-middle, è opportuno prevedere esplicitamente che tutte le comunicazioni avvengano su canali resi sicuri con tecniche crittografiche (SSL, TLS), e che i certificati digitali che asseverano la titolarità dei sistemi hardware e software utilizzati dai partecipanti al

sistema SPID (fornitori di servizi, gestori dell'identità digitale ed eventuali Trusted Third Party) debbano essere emessi da Certificate Authority (CA) che soddisfino dei requisiti definiti dall'AGID e verificati in fase di accreditamento degli Identity Provider e dei Service Provider). Inoltre, l'AGID dovrebbe valutare l'opportunità di rendere disponibile all'utente un client sicuro per l'accesso ai servizi (Secure Browser), con riferimento sia all'ambiente mobile che desktop, ad esempio scaricabile anche dallo stesso sito dell'Agenzia.

Per analoghe motivazioni, nel regolamento recante le "Regole tecniche", al fine di garantire l'identità certa del gestore dell'identità digitale e del fornitore di servizi, la previsione dell'attributo "signature" nelle asserzioni deve essere considerata ovunque obbligatoria e non opzionale.

5.15. Riguardo a quanto previsto dall'art. 26 (Registro SPID), occorre specificare a quali soggetti "appartenenti al circuito SPID" è accessibile il registro predisponendo, ove necessario, modalità selettive di consultazione (v. par. 4.1 dello schema di regolamento recante le regole tecniche). Inoltre, la previsione di "instaurazione di una relazione di fiducia con tutti i soggetti già aderenti, accreditati dall'Agenzia, sulla base della condivisione dei livelli standard di sicurezza dichiarati e garantiti da SPID" in esso contenuta appare troppo generica e ampia: mentre è certamente vero che i Service Provider debbano fare affidamento sugli Identity Provider in una trust relationship, non c'è motivo per cui debba valere il viceversa. Dal punto di vista degli scenari di rischio che andrebbero, come già detto, preventivamente analizzati, il threat model deve includere la possibilità che il fornitore di servizi possa essere di tipo malicious e cerchi di abusare del protocollo per impersonare utenti o gestori dell'identità digitale. In assenza di cautele la presenza di un fornitore di servizi compromesso, anche a seguito di incidente informatico, basterebbe a compromettere l'intero sistema. Per motivi analoghi non va assunta l'esistenza di una automatica relazione di trust tra i vari fornitori di servizi.

5.16. È necessario perfezionare l'articolo 27 (Uso degli attributi SPID) rispetto agli obblighi previsti in materia di protezione dei dati

personali, in relazione a quanto anticipato al punto 5.3. del presente parere.

In tal senso, devono essere soppressi il secondo periodo del secondo comma e il secondo periodo del terzo comma , ferma restando, però, l'esigenza che in entrambi i commi sia previsto che i gestori dell'identità digitale e i fornitori di servizi devono mettere a conoscenza gli utenti degli attributi scambiati, in chiave di correttezza e trasparenza del trattamento dei dati (art. 11, comma 1, lett. a), del Codice) (cfr. punto 5.13).

Infine, l'articolo va integrato con la previsione che i fornitori di servizi possono trattare i dati relativi agli attributi di cui viene richiesta la verifica per il tempo strettamente necessario all'espletamento delle verifiche, cancellandoli al completamento delle stesse.

5.17. Anche l'articolo 28 va perfezionato in relazione agli obblighi previsti in materia di protezione dei dati personali (cfr. punto 5.3.), sopprimendo il terzo comma.

Peraltro non appare condivisibile la prevista comunicazione degli attributi da parte del gestore dell'identità al fornitore di servizi in contesti di autenticazione di livello 1, posto che tale livello non garantisce un alto grado di sicurezza dell'identità asserita (art. 28, parte A) Gestione delle sessioni per il livello 1 SPID; Appendice A).

Inoltre, la previsione per cui "[...] Per il livello 1 SPID è ammessa l'instaurazione di una sessione di autenticazione, associata ad un determinato utente titolare di identità digitale, mantenuta dal gestore dell'identità digitale e condivisa da tutti i fornitori di servizio che nel corso di vita della sessione stessa erogano servizi per quel determinato utente" evidenzia delle criticità, in assenza di misure da parte dei Service Provider, per prevenire i rischi di Cross-Site Request Forgery (XSRF).

Nello stesso articolo 28, in riferimento alle autenticazioni con procedure di Livello 2 SPID, la previsione per cui "[...] 1. 1) il gestore dell'identità digitale non deve mantenere alcuna sessione di autenticazione con l'utente" comporta che l'utente debba effettuare un'autenticazione informatica presso un gestore dell'identità digitale

ogni volta che visiti un nuovo fornitore di servizi. Allo scopo di facilitare l'uso di credenziali di Livello 2 o superiore, potrebbe valutarsi la possibilità di mantenere la sessione di autenticazione con il gestore dell'identità digitale, a condizione che venga chiesta l'autorizzazione all'utente prima di generare ogni nuova asserzione nel contesto di una stessa sessione di autenticazione.

5.18. Agli articoli 28 (Gestione delle sessioni di autenticazione) e 30 (Servizio di discovery) è disciplinato l'utilizzo di cookies per la gestione delle relative sessioni.

L'informazione di stato associata all'utente, anche veicolata attraverso il meccanismo dei cookies, è un'informazione la cui integrità è difficile da garantire, essendo manipolabile, alterabile, cancellabile dall'utente stesso. Appare necessario, pertanto, definire quali siano le funzioni attribuibili al predetto stato.

Nei medesimi articoli si fa riferimento a non meglio specificate "Linee guida indicate dall'Autorità Garante per la protezione dei dati personali".

Si precisa, al riguardo, che il Garante ha adottato il provvedimento "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014" (doc. web n. 3118884 – Pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014) per regolamentare l'utilizzo dei cookie per finalità di profilazione e non sul loro impiego per il mantenimento di una sessione. Si richiede, pertanto, di espungere dagli articoli 28 e 30 ogni riferimento alle "Linee guida indicate dall'Autorità Garante per la protezione dei dati personali".

5.19. Gli articoli 29 e 30 prevedono una "Directory delle identità SPID" alimentata dai gestori delle identità digitali, in cui sono registrate le "informazioni sulle corrispondenze tra gli identificatori delle identità SPID e i relativi gestori", il cui contenuto è reso disponibile ad un "Servizio di Discovery" che consente ai fornitori di servizi di individuare quale gestore dell'identità digitale è in grado di autenticare l'utente. Al riguardo, occorre specificare quale è il

soggetto cui è affidata la gestione e la tenuta dei dati contenuti nella Directory e resi disponibili tramite il Servizio di Discovery.

5.20. L'articolo 31 (Tracciatura e conservazione della documentazione di riscontro) deve essere perfezionato sotto vari profili.

Innanzitutto, al primo comma occorre indicare la normativa di sicurezza a cui ci si riferisce.

Il secondo comma, con un rinvio al comma "2" (e non "4" come previsto ora per un refuso) dell'articolo 13 del dPCM, richiama l'obbligo per i fornitori di servizi di conservare per ventiquattro mesi le informazioni necessarie a imputare, alle singole identità digitali, le operazioni effettuate sui propri sistemi tramite SPID. Tali informazioni sono costituite da registrazioni, il cui insieme costituisce il Registro delle transazioni, disciplinato al comma 3.

Al riguardo, si suggerisce di sostituire il terzo comma con il seguente: "L'insieme delle registrazioni costituisce il Registro delle transazioni del fornitore del servizio. Le tracciature devono avere caratteristiche di riservatezza, inalterabilità e integrità e sono conservate adottando idonee misure di sicurezza ai sensi dell'articolo 31 del decreto legislativo 30 giugno 2003, n. 196, sotto la responsabilità del titolare del trattamento; l'accesso ai dati è riservato a personale espressamente autorizzato e incaricato del trattamento dei dati personali. Devono essere adottati meccanismi di cifratura.".

Il quarto comma, poi, introduce un obbligo di registrazione anche per i gestori dell'identità digitale (non previsto dal dPCM), confermato dalla presenza nelle Regole Tecniche del paragrafo 5 (Tracciatura) che individua le informazioni che i gestori dell'identità digitale dovranno registrare in un apposito Registro delle transazioni. Tali previsioni devono essere coordinate con quelle contenute nel regolamento sui gestori dell'identità digitale.

Coerentemente e per completezza, il predetto paragrafo del regolamento sulle regole tecniche deve essere integrato con le informazioni che i fornitori di servizi devono registrare nel Registro delle transazioni di loro pertinenza.

5.21. É necessario che lo schema sia integrato con disposizioni che assicurino un efficace coordinamento dell'attività di vigilanza e controllo svolte dall'AGID e dal Garante nei rispettivi ambiti e per le finalità istituzionali assegnate, anche in relazione ai casi di "violazione dei dati personali" che hanno riflessi, primariamente se non esclusivamente, sulla protezione dei dati personali, materia di competenza di questa Autorità (cfr. la definizione stessa di "violazione di dati personali" e la relativa disciplina: artt. 4, comma 3, lett. g-bis, e 32-bis del Codice).

Al riguardo, soppresso il penultimo comma dell'articolo 32, dovrebbe essere inserito nello schema un articolo ad hoc, del tenore che a titolo di collaborazione si suggerisce:

"*Art. 32-bis.*
(Collaborazione fra AGID e Garante per la protezione dei dati personali)

1. Nell'ambito delle attività di vigilanza di cui all'articolo 4, comma 1, lett. B), del DPCM sull'operato dei soggetti che partecipano allo SPID, l'AGID, ove riscontri casi in cui sussistano elementi per ritenere la violazione della normativa in materia di protezione dei dati personali, ne informa tempestivamente il Garante per la protezione dei dati personali.
2. Il Garante, anche sulla base delle informazioni di cui al comma 1 o di quelle concernenti violazioni di dati personali di cui all'articolo 4, comma 3, lett. g-bis, del decreto legislativo 30 giugno 2003, n. 196, eventualmente ricevute ai sensi dell'articolo 11, comma 1, lett. o), del DPCM, sottopone a un audit di sicurezza, anche a campione, i soggetti partecipanti allo SPID di cui all'articolo 3, comma 1, lett. a), b) e c) del DPCM, tenuto conto delle diverse categorie dei soggetti interessati. I risultati dell'audit sono inseriti nella relazione annuale del Garante.
3. I gestori dell'identità digitale comunicano al Garante, e per conoscenza all'AGID, la violazione dei dati personali di cui al comma 2 entro 24 ore dall'avvenuta conoscenza della violazione per la prima sommaria comunicazione ed entro 3 giorni dalla stessa per la comunicazione dettagliata. La comunicazione è effettuata mediante

apposito modello predisposto dal Garante e disponibile on line sul sito istituzionale dell'Autorità. Qualora si verifichi una violazione di dati personali e dalla stessa possa derivare un pregiudizio ai dati personali o alla riservatezza di un utente o di altre persone, ossia dei soggetti cui si riferiscono i dati violati, oltre alla comunicazione al Garante i gestori sono tenuti a comunicare l'avvenuta violazione, senza ritardo, anche a tali soggetti, utilizzando il modello predisposto dal Garante. Si applicano, in quanto compatibili, le disposizioni di cui al Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) adottato dal Garante il 4 aprile 2013 e pubblicato sulla Gazzetta ufficiale n. 97 del 4 aprile 2013.
4. Il Garante e l'AGID stipulano un protocollo d'intesa per l'attuazione delle disposizioni del presente articolo nel rispetto delle rispettive competenze.".

IL GARANTE

esprime parere sugli schemi di regolamento dell'Agenzia per l'Italia digitale recanti, rispettivamente, le modalità attuative per la realizzazione dello SPID e le relative regole tecniche, nei termini di cui in motivazione, con le seguenti condizioni:

1) siano valutati i profili di rischio per la sicurezza informatica del sistema SPID illustrati al punto 4;

2) siano apportate agli schemi di regolamento le necessarie modifiche e integrazioni, individuate ai punti da 5.1. a 5.21.

Roma, 4 giugno 2015

IL PRESIDENTE
Soro

RELATORE
Soro

IL SEGRETARIO GENERALE
Busia

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015

in *G. U.* n. 179 del 4 agosto 2015

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO il decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (di seguito Codice);

VISTO il decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (di seguito Cad);

CONSIDERATE le peculiari caratteristiche delle banche dati delle amministrazioni pubbliche, contraddistinte, in particolare, dall'ingente mole di dati trattati, dalla delicatezza delle informazioni ivi contenute e dalla molteplicità di soggetti autorizzati ad accedervi, nonché l'esigenza di garantire costantemente l'esattezza, l'integrità e la disponibilità dei dati personali ivi contenuti non solo in relazione alle c. d. basi dati di interesse nazionale (art. 60 del Cad), unitamente agli specifici rischi di accesso non autorizzato e di trattamento non consentito;

RITENUTO necessario assoggettare il trattamento dei dati personali effettuato nell'ambito delle predette banche dati all'obbligo di comunicazione al Garante del verificarsi di violazioni dei dati o incidenti informatici (accessi abusivi, azione di malware) che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione;

RITENUTO, pertanto, che le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165

debbano comunicare al Garante, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati (c.d. data breach) e che tali comunicazioni devono essere redatte secondo lo schema riportato nell'Allegato 1 al presente provvedimento e inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.pa@pec.gpdp.it;

VISTA, inoltre, la nuova formulazione dell'art. 58, comma 2, del Cad, così come modificato dall'art. 24-quinquies, comma 1, d.l. 24 giugno 2014, n. 90, convertito, con modificazioni, dalla l. 11 agosto 2014, n. 114, in vigore dal 19 agosto 2014, la quale ha previsto che "le pubbliche amministrazioni comunicano tra loro attraverso la messa a disposizione a titolo gratuito degli accessi alle proprie basi di dati alle altre amministrazioni mediante la cooperazione applicativa di cui all'articolo 72, comma 1, lettera e). L'Agenzia per l'Italia digitale, sentiti il Garante per la protezione dei dati personali e le amministrazioni interessate alla comunicazione telematica, definisce entro novanta giorni gli standard di comunicazione e le regole tecniche a cui le pubbliche amministrazioni devono conformarsi";

CONSIDERATO che tale modifica ha superato, quindi, il pregresso impianto normativo relativo all'accessibilità telematica ai dati delle pubbliche amministrazioni, fondato su "apposite convenzioni aperte all'adesione di tutte le amministrazioni interessate volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti"(testo previgente dell'art. 58, comma 2 del Cad);

CONSIDERATO, altresì, che il Garante, nell'ambito del parere del 4 luglio 2013 (doc. web n. 2574977) sulle apposite linee guida dell'Agenzia per l'Italia digitale (di seguito Agid) per la stipula delle predette convenzioni aperte aveva prescritto alle amministrazioni destinatarie delle stesse l'adozione di specifiche misure tecniche e organizzative;

CONSIDERATO che nel trattamento di dati personali l'erogatore (amministrazione titolare del trattamento dei dati personali che mette a disposizione i relativi servizi di accesso) e il fruitore (amministrazione

richiedente che accede in qualità di autonomo titolare ai dati personali resi disponibili dall'erogatore) sono chiamati a rispettare il Codice con particolare riferimento ai presupposti che legittimano i flussi di dati e agli adempimenti in materia di misure di sicurezza;

RITENUTO necessario, pertanto, nelle more della definizione da parte dell'Agid dei suindicati "standard di comunicazione e le regole tecniche", confermare le specifiche misure tecniche e organizzative già individuate, prescrivendo nuovamente l'adozione delle stesse – riportate nell'Allegato 2 al presente provvedimento – al fine di ridurre al minimo i rischi di accessi non autorizzati o di trattamenti non consentiti o non conformi alle finalità della raccolta dei dati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento ai sensi dell'art. 31 del Codice, salvo che le modalità di accesso alle banche dati siano già state oggetto di esame da parte del Garante nell'ambito di specifici provvedimenti;

RILEVATO che le misure necessarie individuate nell'Allegato 2, adeguate al nuovo contenuto del citato art. 58, comma 2, nella sostanza risultano equivalenti a quelle prescritte dal Garante nell'ambito del predetto parere sulle linee guida dell'Agid del 4 luglio 2013;

RITENUTO, pertanto, che le convenzioni già predisposte dalle amministrazioni nel rispetto del richiamato parere del Garante, anche al fine di garantire il rispetto del principio di semplificazione, debbano ritenersi conformi alle misure necessarie individuate nell'Allegato 2 al presente provvedimento;

RITENUTO, invece, che laddove siano state previste modalità di accesso ai dati personali ai sensi della nuova formulazione del predetto art. 58, comma 2 del Cad, non conformi alle misure già individuate dal Garante nel citato provvedimento del 4 luglio 2013, le misure previste nell'Allegato 2 debbano essere adottate dalle amministrazioni interessate entro e non oltre il 31 dicembre 2015;

RILEVATO, infine, che la mancata comunicazione al Garante dei c.d. data breach, nonché la mancata adozione delle misure necessarie

individuate nell'Allegato 2 al presente provvedimento nei suesposti termini e modalità, configurano un illecito amministrativo sanzionato ai sensi dell'art. 162, comma 2-ter del Codice;

VISTA la documentazioni in atti;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la dott.ssa Augusta Iannini;

TUTTO CIÒ PREMESSO IL GARANTE

1. ai sensi dell'articolo 154, comma 1, lett. c), del Codice, prescrive che le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 devono comunicare al Garante, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati e che tali comunicazioni debbano essere redatte secondo lo schema riportato nell'Allegato 1 al presente provvedimento e inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.pa@pec.gpdp.it;

2. ai sensi dell'articolo 154, comma 1, lett. c), del Codice, nelle more della definizione degli "standard di comunicazione e le regole tecniche" da parte dell'Agid ai sensi dell'art. 58, comma 2, del Cad, prescrive alle pubbliche amministrazioni che intendano mettere a disposizione gli accessi alle proprie banche dati alle altre amministrazioni che ne abbiano diritto mediante la cooperazione applicativa di cui all'articolo 72, comma 1, lettera e) del Cad l'adozione delle misure necessarie individuate nell'Allegato 2 al presente provvedimento, salvo che le modalità di accesso alle banche dati siano già state oggetto di esame da parte del Garante nell'ambito di specifici provvedimenti; laddove siano già state previste modalità di accesso ai sensi della nuova formulazione del predetto art. 58, comma 2 del Cad, non conformi alle misure già individuate dal Garante nel provvedimento del 4 luglio 2013, prescrive che le misure necessarie

previste nell'Allegato 2 siano adottate dalle amministrazioni interessate entro e non oltre il 31 dicembre 2015;

3. ai sensi dell'art. 143, comma 2, del Codice dispone la trasmissione di copia del presente provvedimento al Ministero della Giustizia – Ufficio pubblicazione leggi e decreti, per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 2 luglio 2015

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia

ALLEGATI

Allegato 1 – Modello comunicazione data breach

(reperibile all'indirizzo <http://www.garanteprivacy.it/web/guest/ home/docweb/-/docweb-display/docweb/4129029>)

Allegato 2

Misure necessarie

1. Modalità d'accesso

Le pubbliche amministrazioni che intendono rendere fruibili diverse tipologie di dati da altre pubbliche amministrazioni, tenuto conto degli obiettivi di carattere generale perseguiti dal Cad e dell'attuale quadro infrastrutturale disponibile sul territorio, utilizzano le seguenti opzioni tecniche:
- accesso via web, attraverso il sito istituzionale dell'erogatore, un sito tematico appositamente predisposto o altre applicazioni software;

- accesso in modalità di cooperazione applicativa, componente del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

Ferme restando le modalità di accesso telematico definite al punto precedente, che devono considerarsi quelle di riferimento ai fini dell'attuazione delle norme in materia di fruibilità dei dati, le amministrazioni possono utilizzare modalità alternative, laddove si presentino documentabili vantaggi economici o la situazione infrastrutturale e organizzativa non consenta l'adozione di quelle sopra riportate. Le predette circostanze devono essere adeguatamente documentate. In tali casi, le modalità di accesso telematico prevedibili sono:
- la posta elettronica certificata, nei casi specifici, quando la periodicità di acquisizione del dato è limitata (in linea di massima una volta all'anno o meno) e la quantità dei dati da acquisire è contenuta;
- soluzioni di "Trasferimento di File" in modalità FTP "sicuro" o equivalente dal punto di vista della sicurezza del trasporto, qualora preesistenti investimenti, la natura stessa delle richieste e le specifiche condizioni facciano propendere per tale soluzione garantendo la cifratura del canale di trasmissione dei dati (ad esempio, utilizzando meccanismi quali le reti private virtuali o la cifratura delle sessioni di trasferimento dei dati).

2. Presupposti per la comunicazione di dati personali

La convenzione (ovvero qualsivoglia atto bilaterale stipulato tra erogatore e fruitore al fine di stabilire le condizioni e le modalità di accesso ai dati) è lo strumento in cui le amministrazioni possono stabilire le garanzie – anche nei confronti dello stesso erogatore – a tutela del trattamento dei dati personali e dell'utilizzo dei sistemi informativi.

Di seguito vengono pertanto individuati misure e accorgimenti da attuare al fine di assicurare la correttezza del trattamento e di ridurre rischi nell'utilizzo dei dati personali.

In ogni caso l'erogatore, al fine di salvaguardare la sicurezza dei propri sistemi informativi, anche in considerazione delle caratteristiche delle banche dati accessibili attraverso la convenzione, è tenuto a valutare l'introduzione di ulteriori strumenti volti a gestire i profili di autorizzazione, verificare accessi anomali, tracciare le operazioni di accesso, ovvero individuare tassative modalità di accesso alle banche dati, dandone conto nella convenzione (art. 31 del Codice).

2.1 Verifiche preliminari a cura dell'erogatore

L'erogatore prima di stipulare ogni singola convenzione per l'accesso alle proprie banche dati in via telematica deve verificare:
a) la base normativa che legittima il fruitore ad accedere alle proprie banche dati (per i dati diversi da quelli di sensibili e giudiziali: norma di legge o di regolamento, ovvero previa comunicazione al Garante ai sensi dell'art. 19, comma 2 del Codice, qualora manchi una norma di legge o di regolamento e il flusso di dati risulti necessario per lo svolgimento delle proprie funzioni istituzionali; per i dati sensibili e giudiziari: la norma di legge che autorizzi il trattamento e l'individuazione nella stessa, o in atto di natura regolamentare adottato in conformità al parere del Garante, dei tipi di dati e le operazioni eseguibili);
b) la finalità istituzionale perseguita dal fruitore (ad esempio controllo sulle dichiarazioni sostitutive) e la natura e la qualità dei dati richiesti, selezionando accuratamente le informazioni personali contenute nelle banche dati a cui dare accesso;
c) la modalità telematica di accesso alle banche dati più idonea rispetto alle finalità, alla natura e alla quantità dei dati, alle caratteristiche anche infrastrutturali e organizzative del fruitore, al volume e alla frequenza dei trasferimenti, al numero di soggetti abilitati all'accesso.

2.2 Selezione dei dati

La selezione delle informazioni personali oggetto di accesso deve avvenire nel rispetto dei principi di pertinenza e non eccedenza in relazione a ciascuna delle finalità perseguite dal fruitore. Rispetto ad

una medesima banca dati devono essere, infatti, prefigurati diversi livelli e modalità di accesso che offrano al fruitore unicamente i dati necessari per le proprie esigenze istituzionali.

Le modalità di accesso alle banche dati devono essere, pertanto, configurate offrendo un livello minimo di accesso ai dati, anche limitando i risultati delle interrogazioni a valori di tipo booleano (ad es., web services che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un dato oggetto di autocertificazione). Livelli di accesso gradualmente più ampi possono essere autorizzati soltanto a fronte di documentate esigenze del fruitore da indicare in convenzione.

È chiaro, inoltre, che per ciascun fruitore possono essere individuate più modalità di accesso ad una medesima banca dati in relazione alle diverse funzioni svolte dai propri operatori per il perseguimento della medesima finalità, modulando così il livello di accesso ai dati. L'erogatore deve, infatti, far sì che sia consentita, per quanto più possibile, la segmentazione dei dati visualizzabili al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza del fruitore, esclusivamente i dati necessari rispetto alle finalità in concreto perseguite. In altri termini la convenzione deve prevedere l'accesso alle sole informazioni pertinenti e non eccedenti rispetto alla finalità istituzionale perseguita dalla convenzione stessa.

Particolare attenzione deve essere prestata, inoltre, nella scelta delle informazioni richieste per l'interrogazione diretta della banca dati, ovvero per l'invocazione dei web services, imponendo un set minimo di dati per l'individuazione puntuale del soggetto cui si riferiscono. Salvo eccezioni rigorosamente motivate e documentate nella convenzione, la risposta fornita all'interrogazione non deve, poi, contenere un elenco di soggetti.

2.3 Elenco aggiornato

L'erogatore deve poi disporre in ogni momento di informazioni complete e strutturate sui fruitori autorizzati e sulle modalità di accesso alle proprie banche dati.

A tal fine occorre pertanto che l'erogatore rediga un documento, mantenuto costantemente aggiornato, che riporti l'elenco delle banche dati accessibili, descrivendo per ogni fruitore le informazioni di cui ai punti a), b), c), di cui al precedente paragrafo 2.1, corredato delle informazioni relative ai formati dei dati disponibili a fruitori esterni ("tracciato record", schemi XML o altri formalismi).

2.4 Controlli annuali

L'erogatore deve altresì verificare, con cadenza periodica annuale, l'attualità delle finalità per cui ha concesso l'accesso ai fruitori, anche con riferimento al numero di utenze attive, inibendo gli accessi (autorizzazioni o singole utenze) non conformi a quanto stabilito nelle convenzioni.

3. Soggetti incaricati del trattamento

3.1 Designazione responsabili e incaricati

Per effetto dell'esecuzione della convenzione e della conseguente comunicazione dei dati personali, il fruitore, in quanto titolare del trattamento dei dati oggetto di comunicazione da parte dell'erogatore, ai sensi della normativa vigente in materia, deve dare attuazione a quanto previsto dagli artt. 29 e 30 del Codice della privacy, in materia di designazione degli incaricati del trattamento e eventuale designazione del responsabile del trattamento, garantendo che l'accesso ai dati sia consentito esclusivamente a tali soggetti.

Il fruitore si impegna a comunicare all'erogatore, su richiesta motivata, l'elenco degli incaricati del trattamento autorizzati all'accesso ai dati (ad esempio, in caso di controlli sull'attualità delle utenze la cui amministrazione è demandata a gestori presso il fruitore, ovvero nel caso di cooperazione applicativa di cui al punto seguente).

Laddove i fruitori vogliano avvalersi di soggetti terzi (ad esempio, altra pubblica amministrazione o altro soggetto) al fine di realizzare servizi d'interscambio, previa apposita designazione dello stesso soggetto delegato come responsabile o, se persona fisica, anche incaricato del trattamento dei dati personali, devono darne

comunicazione all'erogatore. Tale eventualità deve essere, naturalmente, esplicitamente riportata nella convenzione.

3.2 Procedura di autenticazione e autorizzazione degli utenti

a) Accessi via web

Nel caso in cui la modalità di accesso prescelta preveda l'attribuzione di credenziali individuali (ad esempio, applicazione con accesso interattivo via web), le convenzioni devono predefinire una procedura per il rilascio delle utenze e la gestione delle autorizzazioni degli utenti che coinvolga attivamente le figure apicali degli uffici interessati e un unico supervisore (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore può anche non coincidere con il soggetto tecnicamente deputato alla materiale gestione delle utenze (direttamente o attraverso l'erogatore), ma deve rispondere del controllo sullo stesso.

Nel caso il sistema di accesso preveda la gestione diretta delle utenze da parte del fruitore, la convenzione deve prevedere l'individuazione di uno o più soggetti (coordinati tra loro) deputati alla materiale amministrazione delle utenze di coloro che sono stati autorizzati dal supervisore ad accedere alla banca dati. Tali gestori-amministratori devono essere preferibilmente scelti tra personale che abbia un rapporto stabile con il fruitore e devono essere adeguatamente formati in ordine alle modalità di accesso alla banca dati e all'attività di autorizzazione degli utenti.

Occorre inoltre che venga assicurato un flusso di comunicazione tra il supervisore, il gestore e l'articolazione che si occupa della gestione delle risorse umane, al fine di procedere alla tempestiva revisione del profilo di abilitazione o alla disabilitazione dei soggetti preposti ad altre mansioni o che abbiano cessato il rapporto con l'ente, anche con apposite verifiche a cadenza almeno trimestrale. Il responsabile della convenzione individuato presso il fruitore deve effettuare periodicamente, con cadenza almeno annuale, anche in collaborazione con l'erogatore, una puntuale verifica sulla corretta attribuzione dei profili di autorizzazione e sull'attualità delle utenze attive. Le

convenzioni devono predefinire anche le soglie relative al numero di utenti abilitabili da ciascun fruitore.

L'elenco dei soggetti incaricati da abilitare all'accesso alla banca dati deve essere allegato alla convenzione, ovvero comunicato entro un termine ivi stabilito, e costantemente aggiornato dal responsabile della convenzione. Qualora la gestione degli utenti sia demandata al fruitore, la comunicazione potrà essere limitata agli utenti cui è affidata la funzione di gestori dell'amministrazione delle utenze.

b) Cooperazione applicativa

I web services devono essere integrati soltanto in applicativi che gestiscono procedure amministrative volte al raggiungimento delle finalità istituzionali per le quali è consentita la comunicazione delle informazioni contenute nella banca dati. Devono essere, quindi, possibili unicamente accessi per le finalità per le quali è stata realizzata la convenzione alle sole informazioni pertinenti e non eccedenti rispetto alla finalità istituzionale perseguita dalla convenzione.

In ogni caso, il fruitore deve garantire che i servizi resi disponibili dall'erogatore verranno esclusivamente integrati con il proprio sistema informativo e tali servizi non saranno resi disponibili a terzi per via informatica.

Le modalità di accesso in cooperazione applicativa integrata negli applicativi utilizzati dal fruitore devono assicurare garanzie non inferiori a quelle individuate nel precedente punto a) attraverso idonee policy di sicurezza dei sistemi informativi dello stesso, che prevedano la presenza di una figura apicale (anche coadiuvata da un responsabile tecnico) a garanzia del rispetto dei presupposti per l'accesso stabiliti in convenzione, anche attraverso verifiche periodiche, in termini di:

- gestione delle utenze;

- profili di autorizzazione degli utenti in relazione ai dati ottenuti dall'erogatore mediante la piattaforma del fruitore;

- misure di sicurezza.

Con riferimento all'identificazione dei soggetti incaricati dal fruitore che hanno accesso alla banca dati, al fine di consentire l'adeguato tracciamento delle operazioni compiute sui dati personali, il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata, il codice identificativo dell'utenza che ha posto in essere l'operazione; il suddetto codice identificativo deve essere comunque riferito univocamente al singolo utente incaricato del trattamento che ha dato origine alla transazione; il fruitore, laddove vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato del trattamento direttamente identificabile), deve in ogni caso garantire anche all'erogatore la possibilità, su richiesta, di identificare l'utente nei casi in cui ciò si renda necessario.

3.3 Istruzioni e correttezza del trattamento

Il fruitore deve utilizzare le informazioni acquisite esclusivamente per le finalità dichiarate in convenzione, nel rispetto dei principi di pertinenza e non eccedenza, nonché di indispensabilità, per i dati sensibili e giudiziari.

Il fruitore deve, altresì, garantire che non si verifichino divulgazioni, comunicazioni, cessioni a terzi, né in alcun modo riproduzioni dei dati nei casi diversi da quelli previsti dalla legge, stabilendo le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione. A tal fine il fruitore si impegna ad utilizzare i sistemi di accesso ai dati in consultazione on line esclusivamente secondo le modalità con cui sono stati resi disponibili e, di conseguenza, a non estrarre i dati per via automatica e massiva (attraverso ad esempio i cosiddetti "robot") allo scopo, ad esempio, di velocizzare le attività e creare autonome banche dati non conformi alle finalità per le quali è stato autorizzato all'accesso.

Il fruitore deve garantire, inoltre, che l'accesso ai dati verrà consentito esclusivamente al personale dipendente o a soggetti ad esso assimilati ovvero ad altri soggetti che siano stati parimenti designati dal fruitore quali incaricati o responsabili del trattamento dei dati, impartendo, ai sensi degli artt. 29 e 30 del Codice, precise e dettagliate istruzioni,

richiamando la loro attenzione sulle responsabilità connesse all'uso illegittimo dei dati, nonché al corretto utilizzo delle funzionalità dei collegamenti.

4. Dati sensibili e giudiziari

In ogni caso, qualora sia indispensabile accedere a dati sensibili o giudiziari, questi devono essere opportunamente cifrati con algoritmi che garantiscano livelli di sicurezza adeguati al contesto ai sensi dell'art. 22, comma 6, del Codice.

In considerazione della delicatezza e della quantità di informazioni scambiate, l'erogatore deve individuare le modalità di trasferimento dei dati sensibili e giudiziari maggiormente idonee ad assicurare la sicurezza dei collegamenti, prevedendo che il trasferimento dei dati idonei a rivelare lo stato di salute deve essere in ogni caso cifrato.

5. Misure di sicurezza

Oltre a garantire il rispetto delle misure minime di sicurezza previste dall'artt. 33 e ss. Codice e dal relativo Allegato B, al fine di adempiere agli obblighi di sicurezza di cui all'art. 31 del Codice nella fruibilità dei dati oggetto della convenzione (sia in caso di accessi via web che di cooperazione applicativa), l'erogatore e il fruitore devono assicurare che:

a. gli accessi alle banche dati avvengano soltanto tramite l'uso di postazioni di lavoro connesse alla rete Ip dell'ente autorizzato o dotate di certificazione digitale che identifichi univocamente la postazione di lavoro nei confronti dell'erogatore, anche attraverso procedure di accreditamento che consentano di definire reti di accesso sicure (circuiti privati virtuali);

b. laddove l'accesso alla banca dati dell'erogatore avvenga in forma di web application esposta su rete pubblica (Internet), l'applicazione sia realizzata con protocolli di sicurezza provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali conformi alla norma tecnica ISO/IEC 9594-8:2014,

emessi da una Certification Authority e riconosciuti dai più diffusi browser e sistemi operativi;

c. le procedure di registrazione avvengano con il riconoscimento diretto e l'identificazione certa dell'utente;

d. le regole di gestione delle credenziali di autenticazione prevedano, in ogni caso:

- l'identificazione univoca di una persona fisica;

- processi di emissione e distribuzione delle credenziali agli utenti in maniera sicura seguendo una procedura operativa prestabilita, o di accettazione di forme di autenticazione forte quali quelle che prevedono l'uso di one time password o di certificati di autenticazione (CNS o analoghi);

- che le credenziali siano costituite da un dispositivo in possesso ed uso esclusivo dell'incaricato provvisto di pin o una coppia username/password, ovvero da credenziali che garantiscano analoghe condizioni di robustezza;

e. nel caso le credenziali siano costituite da una coppia username/password, siano adottate le seguenti politiche di gestione delle password:

- la password, comunicata direttamente al singolo incaricato separatamente rispetto al codice per l'identificazione (user id), sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni tre mesi e le ultime tre password non possano essere riutilizzate;

- le password devono rispondere a requisiti di complessità (almeno otto caratteri, uso di caratteri alfanumerici, lettere maiuscole e minuscole, caratteri estesi);

- quando l'utente si allontana dal terminale, la sessione deve essere bloccata, anche attraverso eventuali meccanismi di time-out;

- le credenziali devono essere bloccate a fronte di reiterati tentativi falliti di autenticazione;

f. devono essere sempre presenti misure di protezione perimetrali logico-fisiche, quali ad esempio firewall e reti private virtuali (VPN);

g. i sistemi software, i programmi utilizzati e la protezione antivirus devono essere costantemente aggiornati sia sui server che sulle postazioni di lavoro;

h. le misure di sicurezza devono periodicamente essere riconsiderate ed adeguate ai progressi tecnici e all'evoluzione dei rischi;

i. la procedura di autenticazione dell'utente deve essere protetta dal rischio di intercettazione delle credenziali da meccanismi crittografici di robustezza adeguata;

j. siano introdotti meccanismi volti a permettere il controllo degli accessi al fine di garantire che avvengano nell'ambito di intervalli temporali o di data predeterminati, eventualmente definiti sulla base delle esigenze d'ufficio;

k. in caso di accessi via web deve essere di regola esclusa la possibilità di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse;

l. anche al fine di ottemperare all'obbligo di comunicare al Garante entro 48 ore i casi di data breach, entrambi si impegnano a comunicare tempestivamente:

- incidenti sulla sicurezza occorsi al proprio sistema di autenticazione qualora tali incidenti abbiano impatto direttamente o indirettamente nei processi di sicurezza afferenti la fruibilità di dati oggetto di convenzione;

- ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione on line;

- ogni modificazione tecnica od organizzativa del proprio dominio, che comporti l'impossibilità di garantire l'applicazione delle regole di sopra riportate o la loro perdita di efficacia;

m. tutte le operazioni di trattamento di dati personali effettuate dagli utenti autorizzati, ivi comprese le utenze di tipo applicativo e sistemistico, devono essere adeguatamente tracciate. Al tal fine:

- il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata, il codice identificativo dell'utenza che ha posto in essere l'operazione;

- il suddetto codice identificativo, anche nel caso in cui l'accesso avvenga attraverso sistemi di cooperazione applicativa, deve essere comunque riferito univocamente al singolo utente incaricato del trattamento che ha dato origine alla transazione;

- il fruitore, laddove vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato del trattamento direttamente identificabile), deve in ogni caso garantire anche all'erogatore la possibilità, su richiesta, di identificare l'utente nei casi in cui ciò si renda necessario.

6. Controlli

L'erogatore e il fruitore devono predisporre idonee procedure di audit sugli accessi alle banche dati, i cui esiti devono essere documentati secondo le modalità definite nelle convenzioni.

In particolare, devono essere introdotte attività di audit basate sul monitoraggio statistico delle transazioni e su meccanismi di alert che individuino comportamenti anomali o a rischio.

A tal fine, nelle applicazioni volte all'uso interattivo da parte di incaricati deve essere inserito un campo per l'indicazione obbligatoria del numero di riferimento della pratica (ad es. numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.

Le suddette procedure devono, inoltre, prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso (quali, in particolare, la rispondenza delle interrogazioni ad una precisa finalità amministrativa).

7. Casi particolari

Come sopra ricordato, è compito dell'erogatore valutare l'introduzione di eventuali ulteriori misure e accorgimenti al fine di

salvaguardare la sicurezza dei propri sistemi informativi, anche in considerazione delle caratteristiche delle banche dati accessibili attraverso la convenzione (ad esempio, delicatezza e rilevanza delle informazioni accedute, rilevanti dimensioni della banca dati o del numero di utenti o volume di trasferimenti). Tali misure possono riguardare, in particolare:

- l'individuazione di tassative modalità di accesso alle banche dati;

- la gestione diretta da parte dell'erogatore dei profili di abilitazione, con la conoscenza dei dati identificativi dei soggetti autorizzati all'accesso alla banca dati per la realizzazione delle finalità istituzionali dichiarate nella convenzione;

- l'utilizzo di strumenti di strong authentication per l'autenticazione informatica di particolari categorie di utenti;

in caso di accessi via web o applicazioni software:

- nella prima schermata successiva al collegamento con la banca dati, siano visualizzabili le informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione);

- le informazioni di cui al punto precedente devono essere riportate anche relativamente alla sessione corrente;

- la verifica di accessi anomali attraverso strumenti di business intelligence per monitorare gli accessi attraverso i log relativi a tutti gli attuali e futuri applicativi utilizzati da parte dei fruitori, ovvero attraverso specifiche procedure di audit dell'erogatore presso il fruitore.

Giurisprudenza

CORTE DI CASSAZIONE, sezione Lavoro, sentenza 27 maggio 2015, n. 10955

Non è illegittima la condotta dell'azienda che crea un falso profilo Facebook per dimostrare l'assenza di un dipendente durante l'orario di lavoro.

Svolgimento del processo

1. (OMISSIS), dipendente della (OMISSIS) s.r.l. con la qualifica di operaio addetto alle presse stampatrici, è stato licenziato in data 24 settembre 2012 sulla base delle seguenti contestazioni: 1) in data 21/8/2012 si era allontanato dal posto di lavoro per una telefonata privata di circa 15 minuti che gli aveva impedito di intervenire prontamente su di una pressa, bloccata da una lamiera che era rimasta incastrata nei meccanismi; 2) nello stesso giorno era stato trovato, nel suo armadietto aziendale, un dispositivo elettronico (Ipad) accesso e in collegamento con la rete elettrica; 3) nei giorni successivi, in orari esattamente indicati, si era intrattenuto con il suo cellulare a conversare su face book. Il licenziamento è stato intimato per giusta causa, ai sensi dell'articolo 1, comma 10, Sez., 4 - Tit. 7 del C.C.N.L. di categoria.

1.1. Il (OMISSIS) ha presentato ricorso Legge n. 300 del 1970, ex articolo 18, come modificato dalla Legge 28 giugno 2012, n. 92, articolo 1, comma 42, al Tribunale di Lanciano il quale, con sentenza resa in sede di opposizione contro l'ordinanza con la quale era stata rigettata l'impugnativa di licenziamento, l'ha accolta e ha dichiarato risolto rapporto di lavoro tra le parti con effetto dalla data del licenziamento; ha quindi condannato la società datrice di lavoro a corrispondere al lavoratore un risarcimento del danno pari a ventidue mensilità dell'ultima retribuzione globale di fatto. Il Tribunale ha infatti ritenuto che i fatti contestati al lavoratore, - non essendo

riconducigli a condotte punite dal C.C.N.L. con sanzioni conservative, in ragione della pluralità delle stesse e della loro commissione in un ristretto contesto spaziotemporale -, nondimeno, non integrassero gli estremi della giusta causa o del giustificato motivo soggettivo, con la conseguenza che in base all'articolo 18 cit., comma 5, nel testo modificato, doveva riconoscersi al lavoratore la sola tutela "attenuata" del risarcimento del danno.

1.2. La sentenza è stata reclamata dinanzi alla Corte d'appello dell'Aquila, con impugnazione principale, dal (OMISSIS) e, con impugnazione incidentale, dalla (OMISSIS) s.r.l. e la Corte aquilana, con sentenza depositata in data 12 dicembre 2013 ha rigettato il reclamo principale e accolto quello incidentale, rigettando così l'impugnativa di licenziamento proposta dal ricorrente, che ha poi condannato alla restituzione della somma ricevuta in esecuzione della sentenza reclamata.

1.3. La Corte territoriale ha ritenuto che i fatti addebitati al lavoratore siano stati provati attraverso la deposizione del teste (OMISSIS), responsabile del personale; che l'accertamento compiuto dalla società datrice di lavoro delle conversazioni via internet intrattenute dal ricorrente con il suo cellulare nei giorni e per il tempo indicato – accertamento reso possibile attraverso la creazione da parte del responsabile del personale di un "falso profilo di donna su face book" – non costituisse violazione della Legge n. 300/1070, articolo 4, in difetto dei caratteri della continuità, anelasticità, invasività e compressione dell'autonomia del lavoratore, nello svolgimento della sua attività lavorativa, del sistema adottato dalla società per pervenire all'accertamento dei fatti. Ha quindi proceduto al giudizio di proporzionalità tra i fatti accertati e la sanzione arrogata, ritenendo che si fosse in presenza di inadempimenti che esulano dallo schema previsto dall'articolo 10 del C.C.N.L., in considerazione del fatto che il lavoratore era stato già sanzionato per fatti analoghi nel 2003 e nel 2009 e che tali precedenti erano stati espressamente richiamati nella lettera di contestazione.

1.4. Contro la sentenza il (OMISSIS) propone ricorso per cassazione sostenuto da tre motivi, cui resiste con controricorso la società. Le parti depositano memorie ex articolo 378 c.p.c..

Motivi della decisione

In via preliminare deve rilevarsi che è infondata l'eccezione di inammissibilità del ricorso per cassazione sollevata dalla difesa della (OMISSIS) s.r.l. nella memoria ex articolo 378 c.p.c., sul presupposto che esso sarebbe stato notificato ai sensi dell'articolo 149 c.p.c., l'11 febbraio 2014 (espressamente definito dal notificante, quale "ultimo giorno"), e cioè il sessantunesimo giorno dopo la data di comunicazione della sentenza della Corte aquilana, avvenuta a mezzo PEC il 12 dicembre 2013. In realtà, come si evince dalla stampigliatura in calce al ricorso, apposta dall'ufficiale giudiziario notificatore, l'atto è stato consegnato per la notifica il 10 febbraio 2014, con la conseguenza che il ricorso è tempestivo e, dunque, ammissibile.

1. Con il primo motivo il ricorrente lamenta "la violazione e falsa applicazione della Legge n. 300 del 1970, articolo 4, della Legge n. 300 del 1970, articolo 18, comma 4, e dell'articolo 1175 c.c., in relazione all'articolo 360 c.p.c., comma 1, n. 3, per non essersi dichiarato inutilizzabile il controllo a distanza operato sul lavoratore senza la preventiva e indispensabile autorizzazione". Assume che lo "stratagemma" (così definito dalla corte del merito) adoperato dall'azienda per accertare le sue conversazioni telefoniche via internet durante l'orario di lavoro costituisce una forma di controllo a distanza, vietato dall'articolo 4 dello statuto dei lavoratori, trattandosi peraltro di un comportamento di rilievo penale, oltre che posto in violazione dei principi di correttezza e buona fede previsti dall'articolo 1175 c.c..

1.2. - Il motivo è infondato.

1.3. - È rimasto accertato nella precedente fase di merito che, previa autorizzazione dei vertici aziendali, il responsabile delle risorse umane della (OMISSIS) s.r.l. ha creato un falso profilo di donna su facebook con richiesta di "amicizia" al (OMISSIS), con il quale aveva poi

"chattato in più occasioni", in orari che la stessa azienda aveva riscontrato concomitanti con quelli di lavoro del dipendente, e da posizione, accertata sempre attraverso face-book, coincidente con la zona industriale in cui ha sede lo stabilimento della società.

1.4. – L'articolo 4 dello statuto dei lavoratori vieta le apparecchiature di controllo a distanza e subordina ad accordo con le r.s.a. o a specifiche disposizioni dell'Ispettorato del Lavoro l'installazione di quelle apparecchiature, rese necessarie da esigenze organizzative e produttive, da cui può derivare la possibilità di controllo. È stato affermato da questa Corte che l'articolo 4 "fa parte di quella complessa normativa diretta a contenere in vario modo le manifestazioni del potere organizzativo e direttivo del datore di lavoro che, per le modalità di attuazione incidenti nella sfera della persona, si ritengono lesive della dignità e della riservatezza del lavoratore" (Cass., 17 giugno 2000, n. 8250), sul presupposto – "espressamente precisato nella Relazione ministeriale - che la vigilanza sul lavoro, ancorche' necessaria nell'organizzazione produttiva, vada mantenuta in una dimensione umana, e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro" (Cass., n. 8250/2000, cit., principi poi ribaditi da Cass., 17 luglio 2007, n. 15892, e da Cass., 23 febbraio 2012, n. 2722).

1.5.- Il potere di controllo del datore di lavoro deve dunque trovare un contemperamento nel diritto alla riservatezza del dipendente, ed anche l'esigenza, pur meritevole di tutela, del datore di lavoro di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore.

1.6. - Benché non siano mancati precedenti di segno contrario (Cass., 3 aprile 2002, n. 4746), tale esigenza di tutela della riservatezza del lavoratore sussiste anche con riferimento ai cosiddetti "controlli difensivi" ossia a quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e

non la tutela di beni estranei al rapporto stesso, ove la sorveglianza venga attuata mediante strumenti che presentino quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro" (Cass., n. 15892/2007, cit.; v. pure Cass., 1 ottobre 2012, n. 16622). In tale ipotesi, è stato precisato, si tratta di "un controllo c.d. preterintenzionale che rientra nella previsione del divieto flessibile di cui all'articolo 4, comma 2" (Cass. 23 febbraio 2010 n. 4375).

1.7. - Diversamente, ove il controllo sia diretto non già a verificare l'esatto adempimento delle obbligazioni direttamente scaturenti dal rapporto di lavoro, ma a tutelare beni del patrimonio aziendale ovvero ad impedire la perpetrazione di comportamenti illeciti, si è fuori dallo schema normativo della Legge n. 300 del 1970, articolo 4.

1.8. - Si è così ritenuto che l'attività di controllo sulle strutture informatiche aziendali per conoscere il testo di messaggi di posta elettronica, inviati da un dipendente bancario a soggetti cui forniva informazioni acquisite in ragione del servizio, prescinde dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa ed è, invece, diretta ad accertare la perpetrazione di eventuali comportamenti illeciti (poi effettivamente riscontrati) (Cass., n. 2722/2012). Così come è stata ritenuta legittima l'utilizzazione, da parte del datore di lavoro, di registrazioni video operate fuori dall'azienda da un soggetto terzo, estraneo all'impresa e ai lavoratori dipendenti della stessa, per esclusive finalità "difensive" del proprio ufficio e della documentazione in esso custodita (Cass., 28 gennaio 2011, n. 2117).

1.9. - Infine, è stato precisato che le norme poste dalla Legge 20 maggio 1970, n. 300, articoli 2 e 3, a tutela della libertà e dignità del lavoratore, delimitano la sfera di intervento di persone preposte dal datore di lavoro a difesa dei suoi interessi con specifiche attribuzioni nell'ambito dell'azienda (rispettivamente con poteri di polizia giudiziaria e di controllo della prestazione lavorativa), ma non escludono il potere dell'imprenditore, ai sensi degli articoli 2086 e 2104 c.c., di controllare direttamente o mediante la propria

organizzazione gerarchica o anche attraverso personale esterno – costituito in ipotesi da dipendenti di una agenzia investigativa – l'adempimento delle prestazioni lavorative e quindi di accertare mancanze specifiche dei dipendenti già commesse o in corso di esecuzione, e ciò indipendentemente dalle modalità del controllo, che può avvenire anche occultamente, senza che vi ostino né il principio di correttezza e buona fede nell'esecuzione dei rapporti né il divieto di cui alla stessa Legge n. 300 del 1970, articolo 4, riferito esclusivamente all'uso di apparecchiature per il controllo a distanza (Cass. 10 luglio 2009, n. 16196).

1.10. – Nell'ambito dei controlli cosiddetti "occulti", la giurisprudenza di questa Corte ha avuto modo di affermarne la legittimità, ove gli illeciti del lavoratore non riguardino il mero inadempimento della prestazione lavorativa, ma incidano sul patrimonio aziendale (nella specie, mancata registrazione della vendita da parte dell'addetto alla cassa di un esercizio commerciale ed appropriazione delle somme incassate), e non presuppongono necessariamente illeciti già commessi (Cass., 9 luglio 2008, n. 18821; Cass., 12 giugno 2002, n. 8388; v. Cass., 14 febbraio 2011, n. 3590, che ha precisato che le disposizioni dell'articolo 2 dello statuto dei lavoratori non precludono al datore di lavoro di ricorrere ad agenzie investigative – purché queste non sconfinino nella vigilanza dell'attività lavorativa vera e propria, riservata dall'articolo 3 dello statuto direttamente al datore di lavoro e ai suoi collaboratori –, restando giustificato l'intervento in questione non solo per l'avvenuta perpetrazione di illeciti e l'esigenza di verificarne il contenuto, ma anche in ragione del solo sospetto o della mera ipotesi che illeciti siano in corso di esecuzione; e Cass., 2 marzo 2002, n. 3039 che ha ritenuto legittimo il controllo tramite pedinamento di un informatore farmaceutico da parte del capo area; v. pure Cass., 14 luglio 2001, n. 9576, in cui si è ribadita, citando ampia giurisprudenza, la legittimità dei controlli effettuati per il tramite di normali clienti, appositamente contattati, per verificare l'eventuale appropriazione di denaro – (ammanchi di cassa) – da parte del personale addetto).
In questo stesso orientamento, si pone da ultimo, Cass., 4 marzo 2014, n. 4984, che ha ritenuto legittimo il controllo svolto attraverso

un'agenzia investigativa, finalizzato all'accertamento dell'utilizzo improprio dei permessi ex Legge n. 104 del 1992, ex articolo 33, (suscettibile di rilevanza anche penale), non riguardando l'adempimento della prestazione lavorativa, in quanto effettuato al di fuori dell'orario di lavoro ed in fase di sospensione dell'obbligazione principale di rendere la prestazione lavorativa.

1.11. - Da questo panorama giurisprudenziale, può trarsi il principio della tendenziale ammissibilità dei controlli difensivi "occulti", anche ad opera di personale estraneo all'organizzazione aziendale, in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa, sotto il profilo quantitativo e qualitativo, ferma comunque restando la necessaria esplicazione delle attività di accertamento mediante modalità non eccessivamente invasive e rispettose delle garanzie di libertà e dignità dei dipendenti, con le quali l'interesse del datore di lavoro al controllo ed alla difesa della organizzazione produttiva aziendale deve contemperarsi, e, in ogni caso, sempre secondo i canoni generali della correttezza e buona fede contrattuale.

1.12. - Ad avviso del Collegio, la fattispecie in esame rispetta questi limiti e si pone al di fuori del campo di applicazione dell'articolo 4 dello statuto dei lavoratori. Infatti, il datore di lavoro ha posto in essere una attività di controllo che non ha avuto ad oggetto l'attività lavorativa più propriamente detta ed il suo esatto adempimento, ma l'eventuale perpetrazione di comportamenti illeciti da parte del dipendente, poi effettivamente riscontrati, e già manifestatisi nei giorni precedenti, allorché il lavoratore era stato sorpreso al telefono lontano dalla pressa cui era addetto (che era così rimasta incustodita per oltre dieci minuti e si era bloccata), ed era stata scoperta la sua detenzione in azienda di un dispositivo elettronico utile per conversazioni via internet.
Il controllo difensivo era dunque destinato ad riscontare e sanzionare un comportamento idoneo a ledere il patrimonio aziendale, sotto il profilo del regolare funzionamento e della sicurezza degli impianti. Si è trattato di un controllo ex post, sollecitato dagli episodi occorsi nei giorni precedenti, e cioè dal riscontro della violazione da parte del dipendente della disposizione aziendale che vieta l'uso del telefono

cellulare e lo svolgimento di attività extralavorativa durante l'orario di servizio.

1.13. - Né può dirsi che la creazione del falso profilo face book costituisca, di per sé, violazione dei principi di buona fede e correttezza nell'esecuzione del rapporto di lavoro, attenendo ad una mera modalità di accertamento dell'illecito commesso dal lavoratore, non invasiva né induttiva all'infrazione, avendo funzionato come mera occasione o sollecitazione cui il lavoratore ha prontamente e consapevolmente aderito.

1.14. - Altrettanto deve dirsi con riguardo alla localizzazione del dipendente, la quale, peraltro, è avvenuta in conseguenza dell'accesso a face book da cellulare e, quindi, nella presumibile consapevolezza del lavoratore di poter essere localizzato, attraverso il sistema di rilevazione satellitare del suo cellulare.
In ogni caso, è principio affermato dalla giurisprudenza penale che l'attività di indagine volta a seguire i movimenti di un soggetto e a localizzarlo, controllando a distanza la sua presenza in un dato luogo ed in un determinato momento attraverso il sistema di rilevamento satellitare (GPS), costituisce una forma di pedinamento eseguita con strumenti tecnologici, non assimilabile ad attività di intercettazione prevista dall'articolo 266 c.p.c. e ss., (Cass. pen., 13 febbraio 2013, n. 21644), ma piuttosto ad un'attività di investigazione atipica (Cass., pen., 27 novembre 2012, n. 48279), i cui risultati sono senz'altro utilizzabili in sede di formazione del convincimento del giudice (cfr. sul libero apprezzamento delle prove atipiche, Cass., 5 marzo 2010, n. 5440).

1.14. [1.15. n.d.r.] - Sono invece inammissibili per difetto di autosufficienza le ulteriori doglianze del ricorrente, incentrate sull'inquadrabilità della condotta posta in essere da (OMISSIS), responsabile delle risorse umane della (OMISSIS), e costituita dalla creazione del falso profilo face book, nel reato di cui all'articolo 494 c.p.. Di tale questione non vi è, infatti, cenno nella sentenza impugnata e la parte, pur asserendo di averla sottoposta alla cognizione dei giudici di merito, non indica in quale momento, in quale atto e in quali termini ciò sarebbe avvenuto, con la precisa indicazione dei dati

necessari per il reperimento dell'atto o del verbale di causa in cui la questione sarebbe stata introdotta. Né l'accertamento della rilevanza penale del fatto può essere condotto d'ufficio da questa Corte, poiché la valutazione circa l'esistenza dei presupposti oggettivi e soggettivi del reato richiede un'indagine tipicamente fattuale, che esula dai limiti del sindacato devoluto a questa Corte. Conseguentemente, sono da dichiararsi inammissibili ai sensi dell'articolo 372 c.p.c., i documenti prodotti dal ricorrente unitamente alla memoria difensiva, relativi ad atti del procedimento penale avviato nei confronti del (OMISSIS) (decreto penale di condanna e verbali di interrogatorio), poiché essi non riguardano la nullità della sentenza impugnata né l'ammissibilità del ricorso o del controricorso.

2. Con il secondo motivo il ricorrente censura la sentenza per "violazione e falsa applicazione dell'articolo 2119 c.c., della Legge n. 604 del 1966, articolo 5, dell'articolo 2697 c.c., della Legge n. 300 del 1970, articolo 7, e della Legge n. 300 del 1970, articolo 18, comma 4, in relazione all'articolo 360, comma 1, n. 3), per non essersi assolto all'onere probatorio gravante in capo al datore di lavoro giustificativo del comminato licenziamento. Erronea e carente valutazione delle risultanze probatorie in relazione all'articolo 360, comma 1, n. 5), per essersi erroneamente valutate ed interpretate le acquisizioni probatorie agli atti di causa".

2.1. - Il motivo è inammissibile sotto il profilo della violazione di legge, dal momento che il ricorrente non indica quale affermazione della Corte territoriale si pone in violazione delle norme indicate. Ed invero il vizio di violazione o falsa applicazione di norma di diritto, ex articolo 360 c.p.c., n. 3, deve essere dedotto, a pena di inammissibilità del motivo giusta la disposizione dell'articolo 366 c.p.c., n. 4, non solo con la indicazione delle norme assuntivamente violate, ma anche, e soprattutto, mediante specifiche argomentazioni intelligibili ed esaurienti intese a motivatamente dimostrare in qual modo determinate affermazioni in diritto contenute nella sentenza gravata debbano ritenersi in contrasto con le indicate norme regolatoci della fattispecie o con l'interpretazione delle stesse fornita dalla giurisprudenza di legittimità, diversamente impedendo alla Corte regolatrice di adempiere il suo istituzionale compito di verificare il

fondamento della lamentata violazione. Risulta, quindi, inidoneamente formulata la deduzione di "errori di diritto" individuati per mezzo della sola preliminare indicazione delle singole norme pretesamente violate, ma non dimostrati per mezzo di una critica delle soluzioni adottate dal giudice del merito nel risolvere le questioni giuridiche poste dalla controversia, (cfr. Cass., 8 marzo 2007, n. 5353; Cass., 19 gennaio 2005, n. 1063; Cass., 6 aprile 2006, n. 8106; Cass., 26 giugno 2013, n. 16038; 1 dicembre 2014, n. 25419).

2.2. - Sotto il profilo del vizio di motivazione deve rilevarsi che, nel regime del nuovo articolo 360 c.p.c., comma 1, n. 5, (applicabile ratione temporis alla sentenza in esame, in quanto pubblicata dopo il 30 giorno successivo a quello di entrata in vigore della Legge 7 agosto 2012, n. 134), valgono i principi espressi dalle Sezioni unite di questa Corte, che con la sentenza n. 8053 del 7 aprile 2014, hanno affermato che "L'articolo 360 c.p.c., comma 1, n. 5, riformulato dal Decreto Legge 22 giugno 2012, n. 83, articolo 54, conv. in Legge 7 agosto 2012, n. 134, introduce nell'ordinamento un vizio specifico denunciatile per cassazione, relativo all'omesso esame di un fatto storico, principale o secondario, la cui esistenza risulti dal testo della sentenza o dagli atti processuali, che abbia costituito oggetto di discussione tra le parti e abbia carattere decisivo (vale a dire che, se esaminato, avrebbe determinato un esito diverso della controversia). Ne consegue che, nel rigoroso rispetto delle previsioni dell'articolo 366 c.p.c., comma 1, n. 6, e articolo 369 c.p.c., comma 2, n. 4, il ricorrente deve indicare il "fatto storico", il cui esame sia stato omesso, il "dato", testuale o extratestuale, da cui esso risulti esistente, il "come" e il "quando" tale atto sia stato oggetto di discussione processuale tra le parti e la sua "decisività", fermo restando che l'omesso esame di elementi istruttori non integra, di per sé, il vizio di omesso esame di un fatto decisivo qualora il fatto storico, rilevante in causa, sia stato comunque preso in considerazione dal giudice, ancorché la sentenza non abbia dato conto di tutte le risultanze probatorie".

2.3. - Nel caso di specie, il ricorrente non ha assolto tale onere, avendo omesso di specificare quale tra i fatti principali o secondari non sia stato considerato dal giudice di merito, risolvendosi la censura

essenzialmente nell'addebitare alla Corte di non aver valutato la documentazione esibita dalle parti nel secondo grado del giudizio – documentazione di cui peraltro non viene indicato né il contenuto né i tempi e i luoghi della sua produzione, con evidente violazione del principio di autosufficienza del ricorso per cassazione –; nonché di aver ritenuto provate circostanze di fatto che, invece, non erano state trovate, senza peraltro, anche in tal caso, riportare integralmente le deposizioni testimoniali che non sarebbero state esattamente interpretate e senza specificare dove sarebbero rinvenibili i verbali in cui le dette deposizioni sarebbero state trascritte. Infine, introduce questioni nuove, che non risultano affrontate nella sentenza di merito e rispetto alle quali il ricorrente non fornisce indicazioni sul modo ed il tempo in cui esse sarebbero state introdotte nelle pregresse fasi del giudizio di merito. Ciò vale per la mancata affissione del codice di disciplinare e per la recidiva, che secondo il suo assunto non avrebbe potuto esser utilizzata dal giudice di merito in quanto i fatti, relativi all'anno 2009, sarebbero stati archiviati e gli altri, risalenti al 2003, non potevano certo valere ai fini di determinare il licenziamento.
Con riferimento a quest'ultimo aspetto, è sufficiente rilevare che il giudice del merito ne ha tenuto conto ai soli fini della globale valutazione, anche sotto il profilo psicologico, del comportamento del lavoratore e della gravità degli specifici episodi addebitati, non già come fatto costitutivo del diritto di recesso, con la conseguente irrilevanza dell'asserita archiviazione (Cass., 19 dicembre 2006, n. 27104; Cass., 20 ottobre 2009, n. 22162; Cass., 27 marzo 2009, n. 7523; Cass., 19 gennaio 2011, n. 1145).

2.4. - In definitiva, così impostato, il motivo del ricorso si risolve in un'inammissibile istanza di revisione delle valutazioni effettuate e, in base ad esse, delle conclusioni raggiunte dal Giudice di merito cui non può imputarsi d'avere omesso l'esplicita confutazione delle tesi non accolte e/o la particolareggiata disamina degli elementi di giudizio ritenuti non significativi, giacché soddisfa all'esigenza di adeguata motivazione che il raggiunto convincimento risulti da un esame logico e coerente di quelle tra le prospettazioni delle parti e le emergenze istruttorie che siano state ritenute di per sé sole idonee e sufficienti a

giustificarlo (cfr. tra le tante, Cass., 25 maggio 2006, n. 12446;Cass. 30 marzo 2000 n. 3904; Cass. 6 ottobre 1999 n. 11121).

2.5. - Non sussiste pertanto il denunciato vizio di motivazione il quale, anche nella giurisprudenza precedente all'intervento delle sezioni unite citato, deve emergere dall'esame del ragionamento svolto dal giudice di merito, quale risulta dalla sentenza impugnata, e può ritenersi sussistente solo quando, in quel ragionamento, sia rinvenibile traccia evidente del mancato (o insufficiente) esame di punti decisivi della controversia, prospettate dalle parti rilevabili, ovvero quando esista insanabile contrasto tra le argomentazioni complessivamente adottate, tale da non consentire l'identificazione del procedimento logico-giuridico posto a base della decisione, mentre non rileva la mera divergenza tra valore e significato attribuiti dallo stesso giudice di merito agli elementi da lui vagliati, ed il valore e significato diversi che, agli stessi elementi, siano attribuiti dalla ricorrente e, in genere, dalle parti per tutte, Cass., Sez. Un., 25 ottobre 2013, n. 24148; Cass., ord. 7 gennaio 2014, n. 91).

3. - Con il terzo motivo il ricorrente censura la sentenza per "violazione e falsa applicazione dell'articolo 2119 c.c., della Legge n. 604 del 1966, articolo 1, dell'articolo 1455 c.c., dell'articolo 2697 c.c., e della Legge n. 300 del 1970, articolo 18, comma 4, in relazione all'articolo 360 c.p.c., comma 1, n. 3), sotto il profilo della mancata proporzionalità tra il comportamento addebitato al lavoratore e il licenziamento comminatogli. Violazione e falsa applicazione dell'articolo 2119 c.c., della Legge n. 604 del 1966, articolo 1, degli articoli 9) e 10) sez. 4 , titolo 7 del C.C.N.L. dei metalmeccanici e della Legge n. 300 del 1970, articolo 18, comma 4, in relazione all'articolo 360, comma 1, n. 3), sotto il profilo dell'erronea, incongrua e immotiva applicazione della sanzione del licenziamento comminato al lavoratore".

3.1. - Il motivo è improcedibile con riferimento alla dedotta violazione delle norme del C.C.N.L. dei metalmeccanici, ai sensi dell'articolo 369 c.p.c., comma 2, n. 4, in difetto della produzione, unitamente al ricorso per cassazione, del contratto collettivo, oltre che di ogni precisa indicazione circa il tempo e il luogo della sua produzione nelle

pregresse fasi del giudizio e l'attuale sua collocazione nel fascicolo del giudizio di cassazione.
Quanto al giudizio di proporzionalità, esso è stato condotto dal giudice del merito con rigore, valutando tutti gli elementi di fatto raccolti e complessivamente considerati dai quali ha tratto un giudizio, da un lato, di gravità dei fatti addebitati al lavoratore, in relazione alla portata oggettiva e soggettiva dei medesimi, alle circostanze nelle quali sono stati commessi e all'intensità del profilo intenzionale, dall'altro, di proporzionalità fra tali fatti e la sanzione inflitta, per giungere al convincimento che le lesione dell'elemento fiduciario, su cui si basa la collaborazione del prestatore di lavoro, era tale, in concreto, da giustificare la massima sanzione disciplinare.

4. In definitiva, il ricorso deve essere rigettato, con la condanna del ricorrente al pagamento delle spese del presente giudizio di legittimità, nella misura liquidata in dispositivo.

P.Q.M.

La Corte rigetta il ricorso e condanna il ricorrente al pagamento delle spese del presente giudizio, che liquida in euro 100,00 per esborsi e 4.000,00, per compensi professionali, oltre oneri accessori come per legge.

Ai sensi del Decreto del Presidente della Repubblica n. 115 del 2002, articolo 13, comma 1 quater, da atto della sussistenza dei presupposti per il versamento da parte del ricorrente dell'ulteriore importo a titolo di contributo unificato pari a quello dovuto per il ricorso, a norma del comma 1 bis, dello stesso articolo 13.

CORTE DI CASSAZIONE, sezione I, civile, sentenza 29 maggio 2015, n. 11223

La comunicazione di informazioni sulla salute del dipendente configura un illecito trattamento di dati quando è possibile una comunicazione parziale che contenga il dato pertinente allo scopo da perseguire, mentre va omessa la visibilità di dati sanitari ultronei con particolare riferimento alla patologia da HIV

Svolgimento del processo – Motivi della decisione

1. M.L. ha proposto reclamo al Garante della Protezione dei dati personali lamentando la detenzione da parte del 3 Circolo didattico di (OMISSIS), presso cui era in servizio come insegnante, di copia integrale del verbale relativo all'accertamento sanitario effettuato dalla Commissione medica di verifica di Grosseto, in relazione alla richiesta dell'interessata volta ad ottenere la pensione di inabilità; documento contenente, oltre alla valutazione medico-legale circa l'inidoneità all'impiego, altri suoi dati personali relativi alla diagnosi, agli esami obiettivi e agli accertamenti clinici e strumentali effettuati, nonché informazioni anamnestiche, tra cui quella relativa all'infezione da Hiv, contratta dalla reclamante stessa nel 1987.
Per quanto ancora interessa, il Garante, con *provvedimento del 24.9.2009*, ha evidenziato che il 3 Circolo didattico, in ottemperanza al quadro normativo vigente, stante l'inutilizzabilità dei dati sensibili dell'interessata contenuti nella documentazione trasmessagli dall'organo di accertamento sanitario, avrebbe dovuto astenersi da ogni ulteriore operazione di trattamento dei dati in questione, ad eccezione dell'informazione relativa alla valutazione medico-legale effettuata, adottando ogni misura idonea a limitarne rigorosamente la conoscibilità, senza pregiudicare la prosecuzione del procedimento nel quale era legittimamente coinvolto, essendo destinatario dell'istanza dell'interessata volta ad ottenere la pensione di inabilità (art. 11, comma 1, lett. a) e art. 11, comma 2, del Codice). Per contro il 3 Circolo didattico aveva inviato il verbale, nella sua versione integrale, al 4 Circolo individuato successivamente quale istituzione scolastica

competente ad adottare il provvedimento conseguente all'accertata inabilità al lavoro della M.. Ha, pertanto, ritenuto che la comunicazione al 4 Circolo didattico delle informazioni sulla salute dell'interessata contenute nella versione integrale del verbale di visita collegiale configurava un trattamento illecito di dati, dal momento che il 3 Circolo, avrebbe potuto conseguire ugualmente la prosecuzione del procedimento trasmettendo una copia parziale della documentazione pervenutagli da cui fosse omessa la visibilità di dati sanitari riferiti all'interessata ultronei rispetto a quello dell'accertata inabilità al lavoro e riguardanti la diagnosi accertata, gli esami obiettivi e gli accertamenti clinici e strumentali effettuati, nonchè l'anamnesi da cui emerge anche l'informazione relativa all'Hiv, in maniera tale da rendere nota all'istituzione scolastica competente ad emettere il provvedimento finale soltanto l'informazione relativa al giudizio medico-legale di inidoneità all'impiego (art. 11, comma 2, del Codice; punto 8.4 delle Linee guida).
Adito con ricorso proposto ai sensi del *D.Lgs. n. 196 del 2003, art. 152*, da A.M.L., in proprio e quale dirigente del 3 Circolo, il Tribunale di Grosseto, con sentenza depositata in data 11.11.2010, ha annullato il provvedimento del Garante nella parte in cui aveva ritenuto illecito il trattamento dei dati sensibili da parte del 3 Circolo (in tal senso modificando il dispositivo letto in udienza di totale annullamento del provvedimento).
In sintesi, secondo il giudice del merito la mera trasmissione del documento in maniera riservata non aveva integrato il comportamento di trattamento dei dati sensibili.

1.1. - Contro la sentenza del tribunale M.L. ha proposto ricorso per cassazione affidato a tre motivi. Resiste con controricorso A.M.L. mentre non ha svolto difese il Garante per la protezione dei dati personali.

2.1. - Con il primo motivo la ricorrente denuncia violazione e falsa applicazione dell'art. 4 d.lgs. n. 169/2003 lamentando che il tribunale non abbia ritenuto sussistente l'ipotesi di trattamento di dati sensibili nella trasmissione integrale del documento contenente riferimenti alla patologia da HIV di essa ricorrente.

2.2. - Con il secondo motivo la ricorrente denuncia violazione e falsa applicazione del *D.P.R. 29 ottobre 2001*, del D.Lgs. n. 169 del 2003, artt. 11, comma 1, lett. d, artt. 18 e 20, art. 22, commi 1, 3 e 5, art. 112, commi 1 e 2, lett. d e f, nonchè della *legge n. 135/1990* lamentando che il tribunale abbia escluso l'illiceità della comunicazione della patologia da HIV da parte del dirigente scolastico ad altro Circolo solo per avere apposto la dicitura riservato sulla busta contenente il documento, non ritenendo tenuto il predetto dirigente ad omettere i dati clinici relativi a quella patologia.

2.3. - Con il terzo motivo la ricorrente denuncia vizio di motivazione in ordine al fatto controverso consistente nell'avvenuta diffusione, in ambito scolastico, dei dati sensibili della ricorrente medesima.

3.- I primi due motivi del ricorso sono fondati nei sensi di seguito precisati mentre è inammissibile la terza censura, tendente ad introdurre nel giudizio fatti verificatisi successivamente al provvedimento del Garante. Il D.Lgs. n. 139 [n. 196 n.d.r.] del 2003, art. 11, comma 1, lett. a), dispone che "i dati personali oggetto di trattamento sono… trattati in modo lecito e secondo correttezza" e, al comma 2, che "i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati". A sua volta, il *D.P.R. n. 461 del 2001, art. 4, comma 4,* (Regolamento recante semplificazione dei procedimenti per il riconoscimento della dipendenza delle infermità da causa di servizio, per la concessione della pensione privilegiata ordinaria e dell'equo indennizzo, nonché per il funzionamento e la composizione del comitato per le pensioni privilegiate ordinarie), dispone che "resta fermo quanto previsto dalla *L. 5 giugno 1990, n. 135*, in ordine alle misure anche organizzative da adottare per la tutela della riservatezza in casi di infezione da HIV o di AIDS". Infine, la *L. 5 giugno 1990, n. 135, art. 5,* (Piano degli interventi urgenti in materia di prevenzione e lotta all'AIDS), con la rubrica "Accertamento dell'infezione", dispone, ai commi 4 e 5, che "La comunicazione di risultati di accertamenti diagnostici diretti o indiretti per infezione da HIV può essere data esclusivamente alla persona cui tali esami sono riferiti" e che "l'accertata infezione da HIV non può costituire motivo di discriminazione, in particolare per l'iscrizione alla scuola, per lo

svolgimento di attività sportive, per l'accesso o il mantenimento di posti di lavoro".
La violazione di tale ultima disposizione da parte dell'ente ospedaliero – come correttamente evidenziato dal Garante – aveva reso inutilizzabili quei dati poi trattati dalla resistente.
D'altronde, ai sensi dell'art. 4, lett. 1), codice privacy, si intende per "comunicazione", "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". Come ha rilevato la dottrina, la natura della comunicazione è, quella di una trasmissione a persone determinate dal cui novero, per ovvie ragioni, sono stati esclusi i soggetti innanzi indicati. Sì che, riservata o meno, la mera trasmissione ritenuta non illecita dal tribunale costituiva una comunicazione dei dati. Conclusivamente, vi è stata "comunicazione" di dati sensibili (in precedenza) illecitamente trattati dall'ente ospedaliero (perché non comunicati direttamente all'interessata). Quindi, la resistente ha operato un "trattamento" (con la trasmissione) dei dati illecitamente trattati da altri (art. 4 cit.: "Ai fini del presente codice si intende per: a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti... la comunicazione... di dati").
Ai sensi del *D.Lgs. n. 196 del 2003, art. 22*, poi, i soggetti pubblici conformano il trattamento dei dati sensibili secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato. In particolare, "possono trattare solo i dati sensibili... indispensabili per volgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa".
Talché, correttamente il Garante ha ritenuto che la comunicazione al 4 Circolo didattico delle informazioni sulla salute dell'interessata contenute nella versione integrale del verbale di visita collegiale configurasse un trattamento illecito di dati, dal momento che il 3 Circolo, avrebbe potuto conseguire ugualmente la prosecuzione del procedimento trasmettendo una copia parziale della documentazione pervenutagli da cui fosse omessa la visibilità di dati sanitari riferiti

all'interessata ultronei rispetto a quello dell'accertata inabilità al lavoro e riguardanti la diagnosi accertata, gli esami obiettivi e gli accertamenti clinici e strumentali effettuati, nonché l'anamnesi da cui emerge anche l'informazione relativa all'Hiv, in maniera tale da rendere nota all'istituzione scolastica competente ad emettere il provvedimento finale soltanto l'informazione relativa al giudizio medico-legale di inidoneità all'impiego (per una fattispecie analoga cfr. Sez. 1, n. 10947/2014).

Pertanto, in accoglimento dei primi due motivi del ricorso, la sentenza impugnata deve essere cassata e, non sussistendo necessità di ulteriori accertamenti in fatto, la Corte può decidere nel merito la causa ai sensi *dell'art. 384 c.p.c.*, rigettando l'opposizione proposta dalla A., la quale deve essere condannata al pagamento delle spese processuali del giudizio nella misura determinata in dispositivo.

P.Q.M.

La Corte accoglie il ricorso nei sensi di cui in motivazione, cassa la sentenza impugnata e, decidendo nel merito ai sensi *dell'art. 384 c.p.c.*, rigetta l'opposizione proposta da A.M.L. contro il provvedimento del Garante per la protezione dei dati personali del 24.9.2009. Condanna la resistente al pagamento delle spese processuali che liquida in Euro 7.200,00, di cui Euro 200,00 per esborsi oltre accessori e spese forfettarie come per legge, quanto al giudizio di legittimità e in Euro 3.200,00, di cui Euro 2.000,00 per onorario, oltre accessori di legge, quanto al grado di merito.

Così deciso in Roma, nella Camera di Consiglio, il 29 aprile 2015.

Depositato in Cancelleria il 29 maggio 2015.

Editoriale

Contributi

Rassegna giuridica

ISTITUTO ITALIANO PRIVACY

ISSN 2239 -7671

Anno VI, numero 2, 2015 - Diritto, Economia e Tecnologie della Privacy

€ 25,00