Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante cookies

IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA
Anno XXVIII Fasc. 4-5 - 2012

Alessandro Mantelero

SI RAFFORZA LA TUTELA DEI DATI PERSONALI: *DATA BREACH NOTIFICATION* E LIMITI ALLA PROFILAZIONE MEDIANTE I *COOKIES*

Estratto

MVLTA PAVCIS AG

Milano • Giuffrè Editore

ALESSANDRO MANTELERO

SI RAFFORZA LA TUTELA DEI DATI PERSONALI: *DATA BREACH NOTIFICATION* E LIMITI ALLA PROFILAZIONE MEDIANTE I *COOKIES*

SOMMARIO: 1. Le ragioni del rafforzamento della *data protection* in uno scenario globale ed il ritardo italiano. — 2.1. La mercificazione delle informazioni personali ed il consenso allo sfruttamento dei dati: le disposizioni comunitarie (la c.d. *cookie law*). — 2.2. (*segue*): le norme nazionali di attuazione. — 3. Il valore delle informazioni e le esigenze di contrastare l'accesso illegittimo ai dati.

1. Le ragioni del rafforzamento della *data protection* in uno scenario globale ed il ritardo italiano.

Con il D.Lgs. 69/2012 il Governo, sulla base della delega contenuta nella legge comunitaria 2010[1], ha dato attuazione alle direttive 2009/136/CE[2] e 2009/140/CE[3]. In particolare, limitatamente al tema delle presenti note, la prima delle due direttive ha apportato modifiche alla direttiva 2002/58/CE (c.d. direttiva e-privacy)[4], in-

* Il presente saggio — come gli altri della Sezione — è stato espressamente richiesto dalla Direzione della Rivista per commentare le recenti, importanti, novità legislative in materia di nuove tecnologie dell'informazione. Com'è prassi nei confronti di contributi sollecitati, la revisione è stata effettuata dalla Direzione stessa.

1 Cfr. l'art. 9, L. 15 dicembre 2011, n. 217.

2 Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, in G.U.C.E. L337 del 18 dicembre 2009.

3 Direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica, in G.U.C.E. L 337 del 18 dicembre 2009.

4 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), in G.U.C.E. L 201 del 31 luglio 2002. Salvo diversa indicazione il riferimento alla direttiva 2002/58/CE è al testo consolidato, comprensivo delle modifiche apportate dalla successiva direttiva 2009/136/CE.

cidendo sulle norme in materia di sicurezza del trattamento dati e su quelle concernenti i dispositivi volti ad archiviare informazioni o ad avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente (quali in particolare i « marcatori elettronici », meglio noti come *cookies*).

Con riguardo a tali aspetti il legislatore italiano, mediante il citato decreto, ha apportato significative modifiche al D.Lgs. 196/2003 in materia di protezione dei dati personali, prima di procedere all'esame delle quali occorre tuttavia delimitare il campo applicativo della direttiva 2002/58/CE onde individuare i destinatari delle norme.

Ai sensi dell'art. 3, direttiva 2002/58/CE, quest'ultima si applica solamente al trattamento dei dati personali « connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati », laddove per « servizi di comunicazione elettronica » si intendono i servizi « forniti di norma a pagamento consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche [...], ma ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti; sono inoltre esclusi i servizi della società dell'informazione di cui all'articolo 1 della direttiva 98/34/CE non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica »[5]. A tal proposito l'Article 29 Data Protection Working Party, pronunciandosi sul testo sostanzialmente analogo della proposta di direttiva, ha ritenuto che « chi fornisce contenuti trasmessi utilizzando reti e servizi di comunicazioni elettroniche non rientrerà nell'ambito di applicazione della direttiva modificata sulla vita privata e le telecomunicazioni », specificando inoltre che i fornitori di servizi internet ricadono nell'ambito della direttiva solo nella misura in cui operano in quanto fornitori di accesso e forniscono la connessione a internet, dovendosi invece unicamente guardare alla direttiva generale 95/46/CE quando operano in qualità di fornitori di contenuti[6].

---

[5] Cfr. art. 2 *c*) della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro), in G.U.C.E. L 108 del 24 aprile 2002.

[6] Cfr. Article 29 Data Protection Working Party, *Tutela della vita privata su Internet — Un approccio integrato dell'EU alla protezione dei dati on-line* —, documento di lavoro adottato il 21 novembre 2000, 28; tutti i documenti adottati dall'Article 29 Data Protection Working Party richiamati nel presente contributo sono consultabili al seguente indirizzo: *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*. In merito alla natura « a pagamento » della fornitura dei servizi, lo stesso Working Party ha precisato che « nella giurisprudenza della Corte europea di giustizia è stato chiarito che, con riguardo ai servizi ai sensi dell'articolo 50 (*ex* articolo 60) del trattato CE, il compenso non deve essere necessariamente corri-

Analogamente è stato rilevato come le disposizioni della direttiva non riguardano neppure i motori di ricerca né i *social network*, salvo le ipotesi in cui questi offrano servizi supplementari rientranti nel campo di applicazione della direttiva (es. servizio di posta elettronica)[7].

Alla luce del *wording* della direttiva e dei richiamati rilievi interpretativi, si deve dunque ritenere che le disposizioni in materia di *data breach* di cui all'art. 4, direttiva 2002/58/CE, in quanto riferite al « provider of a publicly available electronic communications service », non riguardino né i fornitori di contenuti né i motori di ricerca o i gestori dei *social network*, fatte salve le precisazione anzidette[8].

Diversamente, le previsioni concernenti i dispositivi volti ad archiviare informazioni o ad avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente[9] hanno un ambito di applicazione più ampio, tale da estendersi anche all'erogazione di servizi *on-line* diversi da quelli di cui all'art. 2 *c*), direttiva 2002/21/CE[10]. Come infatti precisato anche nel considerando n. 24 della direttiva 2002/58/CE[11] le apparecchiature terminali degli utenti rientrano nel contesto della sfera privata di quest'ultimi, ne consegue che la tutela riconosciuta a tale ambito[12] limita in maniera estensiva l'adozione di sistemi di monitoraggio delle attività poste in essere *on-line* da parte degli utenti.

---

sposto dal fruitore del servizio ma può essere corrisposto, ad esempio, dalle società pubblicitarie. Nel caso di un fornitore di accesso gratuito, chi pubblica annunci o banner pubblicitari nelle pagine Internet offre di fatto un compenso al fornitore in questione ». Cfr. altresì Article 29 Data Protection Working Party, *Parere 2/2008 sul riesame della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*, adottato il 15 maggio 2008, 3.

[7] Cfr. Article 29 Data Protection Working Party, *Parere 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca*, adottato il 4 aprile 2008, 12, e Article 29 Data Protection Working Party, *Parere 5/2009 sui social network on-line*, adottato il 12 giugno 2009, 11.

[8] Cfr. in tal senso anche Garante per la protezione dei dati personali (in seguito Gar.), Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali, 26 luglio 2012, doc. web n. 1915485, punto 3; cfr. inoltre già nello stesso senso Gar., Sicurezza dei dati di traffico telefonico e telematico, provvedimento del 17 gennaio 2008, doc. web n. 1482111. Tutti i provvedimenti del Garante per la protezione dei dati personali richiamati nel presente contributo sono consultabili al seguente indirizzo: *www.garanteprivacy.it*.

[9] Cfr. art. 5.3 direttiva 2002/58/CE.

[10] Cfr. Article 29 Data Protection Working Party, *Parere 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca*, cit., 13, secondo cui « Alcune disposizioni della direttiva, come l'articolo 5, paragrafo 3 (cookie e spyware) e l'articolo 13 (comunicazioni indesiderate), sono disposizioni generali applicabili non soltanto ai servizi di comunicazione elettronica, ma anche ad ogni altro servizio che si avvalga di tali tecniche ».

[11] Nel considerando n. 24 si legge: « terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms ».

[12] Cfr. art. 7 della Carta dei Diritti Fondamentali dell'Unione Europea.

Individuati i destinatari delle disposizioni recepite nel nostro ordinamento con il D.Lgs. 69/2012, va rilevato come al fine dell'analisi delle modifiche apportate al D.Lgs. 196/2003 non sia sufficiente dar semplicemente conto delle nuove norme introdotte e dei conseguenti obblighi, ma occorra invece contestualizzare tali interventi nel più generale panorama delle dinamiche inerenti la circolazione dei dati personali ed il loro sfruttamento per finalità commerciali, alla luce delle linee di riforma emergenti in tale ambito sia in Europa che in diverse altre aree geografiche (Stati Uniti *in primis*).

Va infatti sottolineato come la percezione della rilevanza dei problemi cui le norme in esame cercano di dare risposta sia ormai diffusa a livello globale, seppur le soluzioni operative approntate vengano declinate in maniera differente nei vari contesti[13]. Nello specifico, i due temi centrali su cui verte la recente novella, ovvero la profilazione degli utenti durante la navigazione *on-line* e la gestione degli eventi di *data breach*, costituiscono aspetti da tempo posti all'attenzione dei regolatori[14], in ragione del crescente valore in chiave strategica e predittiva assunto dalle informazioni — ed in particolare da quelle personali — nelle economie più avanzate[15].

La spinta a fornire servizi sempre più ritagliati sulle preferenze del singolo cliente ha infatti indotto già da alcuni decenni ad affinare le tecniche di *direct marketing* che hanno trovato nella digitalizzazione e nella diffusione dell'utilizzo della rete internet un importante fattore di sviluppo[16]. A tal fine, onde incrementare le proprie possibilità di collocare beni e servizi ed acquisire un vantaggio competitivo rispetto ai concorrenti, le imprese necessitano di molte informazioni sulle abitudini personali e sulle preferenze del singolo, in diversi casi neppure in diretta e stretta correlazione con quanto offerto. Ne consegue che molte società hanno negli anni via via incrementato le proprie basi di dati, affinando i profili dei clienti già acquisiti e di quelli potenziali. Dopo decenni di raccolta ed analisi delle informazioni è evidente come quelli posseduti non siano più semplici dati, ma costituiscano un vero e pro-

---

[13] Rispetto a queste generali tendenze di riforma e di rafforzamento della tutela dei dati personali l'atteggiamento del legislatore italiano, negli ultimi anni, è tuttavia parso meno sensibile, come comprovato anche dalla tardiva attuazione delle modifiche introdotte dalla direttiva 2009/136/CE.

[14] Prova ne sia il fatto stesso che le direttive oggetto di attuazione risalgono al 2009.

[15] Sia consentito a tal riguardo, stante l'economia del presente scritto, rinviare alle considerazioni più ampiamente formulate in proposito ed alla letteratura richiamata in A. Mantelero, Big Data*: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in questa *Rivista*, 2012, 135 ss.

[16] Cfr. J. Turow, *Niche Envy: Marketing Discrimination in the Digital Age*, Cambridge (Mass.)-London, 2006 ed altresì P.M. Schwartz-D.J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 *New York University Law Review* 1814, 1848-64 (2011).

prio *asset* strategico di notevole valore, in proporzione dell'ampiezza e della qualità delle informazioni raccolte.

In questo scenario l'evoluzione tecnologica ha aperto nuove vie alla profilazione degli individui, attraverso il monitoraggio delle loro attività nel contesto *on-line*[17], laddove la persona esprime in molteplici modi il proprio essere ed addirittura in vari casi svela aspetti altrimenti celati, forte di un presunto anonimato dell'agire nella Rete. Ne consegue che i vari gesti quotidiani di *point-and-click* e di ricerca *on-line* disvelano passioni politiche, gusti letterari, patologie e molte altre componenti del nostro carattere.

Negli ultimi anni rispetto a tali attività di profilazione è stata introdotta un'ulteriore variabile correlata alla progressiva concentrazione dei servizi *on-line* di più frequente uso da parte degli utenti. L'iniziale pluralismo di soluzioni, nato dalla creatività dei singoli, ha infatti lasciato il campo a pochi *big players* che dominano in specifici ambiti di mercato, è il caso di Google e Bing fra i motori di ricerca, di Facebook (e Google) nei *social network*, di eBay nelle vendite *on-line* e di alcuni (non molti) altri operatori detentori di quote assai significative di mercato nell'offerta di diversi fra i più popolari servizi. L'accentramento delle forme di profilazione in capo ad uno o pochi operatori, rispetto a ciascun ambito, che ne è conseguito permette alle grandi società dell'IT di superare l'iniziale modello incentrato sulla profilazione individuale per estenderlo ad analisi di rete o di gruppo. Diviene così possibile trarre inferenze predittive sui comportamenti di specifici *cluster* di soggetti definiti secondo criteri di appartenenza sociale, geografica, politica o in ragione delle relazioni esistenti far i membri del *network*. Si è passati in questo modo dalla definizione di profili individuali a quella di profili di massa.

Questa evoluzione spiega anche come tali forme di analisi non interessino unicamente ai privati, ma anche ai governi, che, se da un lato tradizionalmente abbisognano di informazioni dettagliate sul singolo per erogare i propri servizi relativi allo stato sociale e, più recentemente, quelli di *e-government*, nello stesso tempo sono interessati al potenziale predittivo per scopi di controllo sociale[18] che i c.d. *big data*[19] racchiudono in sé.

---

[17] Sulla natura di dato personale delle informazioni raccolte attraverso il tracciamento *on-line* cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Parere 2/2010 sulla pubblicità comportamentale online*, adottato il 22 giugno 2010, 3. Sulle specifiche tecniche inerenti il funzionamento della principale modalità di tracciamento *on-line*, realizzata mediante il ricorso ai c.d. *cookies*, cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY, *ult. op. cit.*, 6 s.

[18] Si pensi ai programmi statunitensi « Total Information Awareness program », « Novel Intelligence from Massive Data » e « Open Source Indicators Program », cfr. MANTELERO, Big Data*: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., 139, nota 8, ed alle più recenti misure di monitoraggio contenute nel Communications Data Bill inglese, cfr. *http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf*.

[19] Cfr. *supra* nota 15.

A tali sviluppi sul fronte della raccolta dei dati si sono accompagnate, in tempi più recenti, innovazioni tecnologiche su quello della gestione delle informazioni. Proprio l'analisi delle grandi masse di dati cui si è accennato è infatti resa possibile dalla grande potenza di calcolo e di archiviazione disponibile e dal relativamente basso costo della stessa, evoluzione cui il fenomeno del *cloud computing* ha recentemente concorso. La creazione di grandi *data center* implica tuttavia un'ovvia concentrazione spaziale delle informazioni, certamente all'interno di strutture notevolmente protette e soggetta a prassi che garantiscono un'adeguata ridondanza[20], purtuttavia la logica dell'accentramento rende tali *data center* obiettivi assai appetibili per gli autori dei furti di dati. Se infatti le informazioni hanno un valore commerciale per le imprese, se sono divenute merce di scambio fra le stesse e (in parte) fra imprese e clienti, va da sé che esse risultano anche appetibili a coloro che sono mossi dall'intento di conseguire un profitto illecito o di porre in essere pratiche di concorrenza sleale, ovvero, in un diverso ambito, sono animati da fini politici in nome dei quali dar luogo a vere e proprie guerre informatiche fra stati.

Dall'esame del contesto sin qui sommariamente descritto, si coglie la ragion per cui i profili concernenti le modalità di raccolta dei dati e di conservazione degli stessi assumono tanta importanza e si comprende come la regolamentazione di tali aspetti sia destinata ad incidere in maniera significativa non solo sulla tutela dei singoli e dei gruppi, ma anche sugli interessi di chi è intento a sfruttare economicamente tali informazioni. Da qui la difficoltà nel definire le regole che governano la materia, in un territorio di confine dove si intersecano le esigenze di protezione degli individui, gli interessi lobbistici delle imprese di settore, le posizioni — più lungimiranti — di alcuni operatori che vedono nella *data protection* anche un vantaggio competitivo, la volontà degli stati di garantire un ecosistema informativo efficiente e sicuro.

Non è dunque un caso, stante la natura sovranazionale dei mezzi adoperati per la raccolta dei dati, la connotazione multinazionale delle società maggiormente coinvolte e gli interessi degli stati, che le istanze in esame siano emerse in tutte le nazioni ove l'economia digitale si è andata affermando. Certamente le diversità di approccio politico nella tutela dei dati personali (si pensi al forte e repressivo controllo statale esistente in diverse nazioni dell'Asia ed al modello dell'UE), così come le diverse visioni rispetto al rapporto fra dati come merce e come aspetto della personalità (è il caso del confronto fra Stati Uniti ed Unione Europea) mostrano, pur nella sin eccessiva semplificazione qui accennata,

[20] Per ridondanza si intende la disponibilità di diversi apparati per adempiere allo svolgimento della medesima funzione, in maniera che il venire meno del funzionamento di uno o più di tali apparati non sia comunque in grado di pregiudicare il funzionamento dell'intero sistema.

come il bilanciamento fra le opposte esigenze possa conseguirsi in diverse maniere. Tuttavia la natura comune degli interessi in gioco consente di avviare proprio su queste esigenze generalmente avvertite un dialogo fra i vari modelli regolatori, al fine di facilitarne la convergenza verso soluzioni condivise.

Non è dunque un caso che le recenti linee di riforma in materia di *data protection* delineatesi nella UE e le *guidelines* dell'amministrazione statunitense, pur nella diversità di approccio su alcuni aspetti, mostrino la comune volontà di regolare proprio gli accessi illegittimi ai dati e la profilazione degli utenti.

Conferme nel senso di una convergenza su questi temi vengono anche dagli stessi operatori commerciali, come dimostrato, con riguardo alla profilazione *on-line*, dalle iniziative sulla soluzione tecnica del c.d. *Do Not Track*, riguardante l'*advertising on-line* e correlata all'attività dei *browser*, di cui si dibatte sin dagli inizi del 2011[21]. Adottando un approccio orientato alla c.d. *privacy by design*, i principali operatori del settore dei motori di ricerca hanno così offerto una prima risposta di tipo tecnologico[22] alle crescenti preoccupazioni degli utenti concernenti l'*on-line tracking* ed il *behavioral advertising*[23].

---

[21] Cfr., *ex multis*, N. Kroes, *Why we need a sound Do-Not-Track standard for privacy online*, in *http://blogs.ec.europa.eu/neelie-kroes/donottrack/*. A tal riguardo va tuttavia osservato come assuma rilevanza l'impostazione adottata di *default* dal *browser*: ove infatti la funzione anti-tracciamento sia attivabile solo volontariamente dall'utente, di *default* l'utilizzo del *browser* consentirà il tracciamento, viceversa operando in maniera opposta l'utente non sarà profilato salvo che non lo scelga consapevolmente. È evidente che le due soluzioni non sono affatto indifferenti per i pubblicitari, essendo noto che una percentuale assai significativa di utenti non si cura di modificare il *setting* di *default* del *browser*, da qui l'interesse per gli operatori del *marketing* per una funzione « do not track » di *default* disattivata. In tal contesto il World Wide Web Consortium (W3C), l'ente che definisce gli standard per i protocolli internet e le linee guida, ha assunto una posizione affine agli interessi delle grandi imprese del *marketing* diretto auspicando la non attivazione di *default* dell'opzione « do not track ». Tale posizione ha aperto un contrasto con la società Microsoft che ha invece espresso l'intenzione di rilasciare la prossima versione del proprio *browser* (Microsoft Internet Explorer 10), uno dei più utilizzati al mondo, con la funzione « do not track » abilitata di *default*; cfr. B. Lynch (Chief Privacy Officer, Microsoft), *Do Not Track in the Windows 8 Setup Experience*, 7 agosto, 2012, in *http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/08/07/do-not-track-in-the-windows-8-set-up-experience.aspx*.

[22] Nello specifico si tratta dell'incorporazione nell'*header* del *browser* di un'informazione diretta ai siti oggetto di navigazione da parte dell'utente con cui si notifica a quest'ultimi l'intenzione di non essere fatti oggetto di profilazione attraverso tracciamento *on-line*. Questa soluzione, pur essendo più efficiente di altre (come quelle incentrate sui *do-not-track cookies* o su *blacklists*), presenta il limite evidente di veder vincolata la propria efficienza alla disponibilità dei gestori dei siti web di tener conto delle indicazioni ricevute dall'utente tramite il *browser*, nonché dall'eventualità di una sua applicazione solamente parziale, limitata ad alcune tipologie di *cookies*, cfr. Article 29 Data Protection Working Party, *Opinion 4/2012 on Cookie Consent Exemption*, adottata il 7 giugno 2012, 10. Cfr. sull'argomento le osservazioni del Vice-Presidente della Commissione Europea e Commissario per l'Agenda Digitale europea N. Kroes, *Online privacy - reinforcing trust and confidence*, Brussels, 22 June 2011, in *http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/461*.

[23] Il *behavioral advertising* (pubblicità comportamentale) consiste nel traccia-

Dal quadro qui sinteticamente delineato al fine di collocare nel contesto pertinente le recenti modifiche del D.Lgs. 196/2003, si evince da ultimo un ulteriore elemento, consistente nella diversa velocità con cui il panorama italiano, ma soprattutto la classe politica ed imprenditoriale che lo influenza, si muove rispetto alla riflessione in corso in ambito europeo e globale. In particolare il nostro legislatore non solo giunge spesso fra gli ultimi nel recepire le direttive comunitarie in materia, ma soprattutto all'impulso normativo viene sovente a mancare l'affiancamento di un'attività di facilitazione nell'attuazione in favore dei soggetti obbligati[24] e di un'incisiva attività di controllo circa il rispetto delle disposizioni di legge.

2.1. La mercificazione delle informazioni personali ed il consenso allo sfruttamento dei dati: le disposizioni comunitarie (la c.d. *cookie law*).

La trasformazione delle informazioni da semplice elemento funzionale ad un determinato processo in valore economico e strategico ne ha comportato la progressiva patrimonializzazione e disponibilità all'interno degli scambi commerciali. In conseguenza del valore assunto dalle informazioni personali è emersa anche una crescente istanza dei singoli di divenire partecipi e non rimanere meri soggetti passivi di tali scambi, da qui nei diversi ordinamenti il crescente ruolo attribuito alla volontà dell'individuo nel regolare la circolazione dei dati che lo riguardano. Anche qui poi le differenti culture giuridiche di appartenenza hanno portato gli ordinamenti a qualificare diversamente tale circolazione, accentuandone i profili dispositivi e di scambio in taluni contesti e privilegiando invece una visione incentrata sulla persona ed i suoi attributi in altri[25].

---

mento degli utenti durante la navigazione *on-line*, cui consegue la creazione progressiva di profili individuali che vengono successivamente utilizzati per fornire agli utenti contenuti pubblicitari che rispondono ai loro interessi. Cfr. Article 29 Data Protection Working Party, *Parere 2/2010 sulla pubblicità comportamentale on-line*, cit. ed Article 29 Data Protection Working Party, *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, adottata l'8 settembre 2011.

[24] Cfr. invece l'esperienza inglese, *infra* nota 67.

[25] Con riguardo alla dottrina statunitense cfr., *ex multis*, P.M. Schwartz, *Privacy and Democracy in Cyberspace*, in 52 *Vand. L. Rew.* 1609, 1633-34 (1999); J.R. Reindenberg, *Privacy in the Information Economy: A Fortress of Frontier for Individual Rights?*, in 44 *Fed. Comm. L.J.* 195 (1992); R.A. Posner, *The Right of Privacy*, in 12 *Ga. L. Rev.* 393 (1978), consultabile in *http://digitalcommons.law.uga.edu/lectures_pre_arch_lectures_sibley/22*. Con riferimento alla dottrina italiana, sul tema generale degli atti dispositivi sugli attributi della personalità cfr. G. Alpa-G. Resta, *Le persone fisiche e i diritti della personalità*, in *Trattato di Diritto Civile*, diretto da R. Sacco, Torino, 2006, 629 ss.; V. Zeno-Zencovich, *Profili negoziali degli attributi della personalità*, in questa *Rivista*, 1993, 545 ss. e D. Messinetti, *Circolazione dei dati personali e dispo-*

Rispetto alla complessità dei fenomeni di raccolta e delle modalità di elaborazione di dati la sola volontà del singolo, ancorché libera ed elaborata sulla base di adeguate informazioni preventive, può risultare tuttavia inadeguata in ragione della sproporzione esistente in termini di conoscenza e comprensione della complessità e di effettiva libertà di autodeterminazione. Così il singolo utente[26] difficilmente è in grado di cogliere le potenzialità analitiche detenute da chi raccoglie i dati che lo riguardano e nel contempo non può dirsi completamente libero quando, stante la suddetta limitatezza degli operatori che forniscono i singoli servizi, l'alternativa cui si trova sovente di fronte è fra cedere i propri dati o rinunciare a fruire di servizi, quali ad esempio i *social network*, rilevanti per le ragioni sociali ed abilitanti nell'attuale società digitale. Da qui la necessità avvertita dai legislatori di affiancare alla centralità del consenso la creazione di specifiche autorità di controllo in grado di avere quella capacità di analisi e di supervisione che il singolo non può avere ed in grado di incidere sulle politiche adottate dalle grandi imprese dell'ICT.

In tal senso vanno lette le disposizioni in materia di *data protection* adottate nell'UE, a far data della direttiva 95/46/CE. Proprio con riguardo a quest'ultima, già in essa si trova una prima generica risposta alle pratiche intrusive del *marketing* diretto *on-line*, laddove le previsioni inerenti l'informativa all'interessato ed il ruolo del consenso di quest'ultimo offrono un indubbio fondamento per subordinare e suddette pratiche commerciali al coinvolgimento diretto e consapevole del destinatario delle stesse.

Le forme di tracciamento e profilazione correlate alla navigazione *on-line* hanno poi trovato esplicita e più compiuta disciplina nell'ambito della direttiva 2002/58/CE, specie in seguito alle modifiche apportate dalla successiva direttiva 2009/136/CE. Nel dettaglio l'art. 5.3 della direttiva 2002/58/CE nella sua attuale formulazione[27] prevede che l'archiviazione di informazioni oppure l'ac-

sitivi di regolazione dei poteri individuali, in *Riv. crit. dir. priv.*, 1998, 353. In merito ai profili circolatori dei dati personali cfr. altresì: A. Orestano, *La circolazione dei dati personali*, in *Diritto alla riservatezza e circolazione dei dati personali*, vol. II, a cura di R. Pardolesi, Milano, 2003, 119 ss.; G. Pino, *Teorie e dottrine dei diritti della personalità. Uno studio di meta-giurisprudenza analitica*, in *Mat. storia della cult. giurid.*, 2003, 237 ss.; A. di Majo, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in *Trattamento dei dati e tutela della persona*, a cura di V. Cuffaro-V. Ricciuto-V. Zeno-Zencovich, Milano, 1998, 228 ss.; G. Oppo, *Sul consenso dell'interessato*, in *Trattamento dei dati e tutela della persona*, *ivi*, 123 ss.; S. Patti, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999, II, 455 ss.; F. Cafaggi, *Qualche appunto su circolazione, appartenenza e riappropriazione nella disciplina dei dati personali*, in *Danno e resp.*, 1998, 625; V. Zeno-Zencovich, *Una lettura comparatistica della L. n. 675/96 sul trattamento dei dati personali*, in *Riv. trim. dir. e proc. civ.*, 1998, 741.

[26] Nel corso del presente contributo il termine utente è impiegato con il significato di utilizzatore della rete internet ed in generale dei servizi attraverso la stessa erogati.

[27] La formulazione originaria dell'art.

cesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente è consentito solamente ove « l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva 95/46/CE, tra l'altro sugli scopi del trattamento ».

Occorre in proposito tener presente come la nozione di « informazioni » (archiviate o da archiviarsi nell'apparecchiatura terminale dell'utente) deve intendersi in senso esteso, non circoscritta solamente a quelle che abbiano carattere di dati personali, poiché l'aspetto rilevante non è l'informazione in sé, bensì la sfera privata che viene individuata nell'ambito di impiego del dispositivo di comunicazione[28]. La direttiva 2002/58/CE, nel testo emendato, offre dunque una tutela più ampia di quella in precedenza desumibile dalla direttiva 95/46/CE, in base alla quale occorreva la sussistenza di un legame fra la tecnologia intrusiva ed il trattamento di informazioni relative all'utente, mentre adesso è sufficiente il semplice impiego di tali tecnologie perché trovino applicazione le tutele consistenti nell'informativa preventiva e nella previa acquisizione del consenso dell'interessato.

Va per altro osservato come, rispetto alle forme di profilazione commerciale *on-line*, le informazioni memorizzate abbiano sovente carattere personale sia in ragione delle modalità operative dei marcatori, sia in conseguenza delle modalità d'uso dei dispositivi elettronici. Quanto alle prime infatti la pubblicità comportamentale realizzata mediante l'impiego dei *cookies* consente di identificare in maniera univoca il terminale su cui il *cookie* è stato archiviato, ne consegue che è possibile definire un profilo del soggetto che utilizza tale macchina e, successivamente, abbinarlo ad una persona reale quando questi compili ad esempio un *format online* o si registri su un sito affiliato alla rete di *advertising* da cui il *cookie* proviene. Questa conclusione volta a riconoscere il carattere personale di dette informazioni[29], sebbene condivisa a livello comunitario, sembra però non tener conto della possibilità

5.3 direttiva 2002/58/CE era infatti differente dall'attuale in quanto adottava l'opposto modello del c.d. *opt-out*, prevedendo l'obbligo di informare l'utente, ma non il consenso preventivo dello stesso alla memorizzazione di *cookies* e simili, riconoscendo invece il solo diritto di opporsi a tale trattamento (« the right to refuse such processing »).

[28] Cfr. direttiva 2002/58/CE, considerando n. 24, secondo cui « le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente ». Tale interpretazione ha trovato conferma in ARTICLE 29 DATA PROTECTION WORKING PARTY, *Parere 2/2010 sulla pubblicità comportamentale online*, cit., 9 s. e ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, cit., 8.

[29] Cfr. a riguardo ARTICLE 29 DATA PROTECTION WORKING PARTY, *Parere 2/2010 sulla pubblicità comportamentale online*, cit., 10, ed ARTICLE 29 DATA PROTECTION WORKING PARTY, *Parere 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca*, cit., 9.

che più utenti utilizzino il medesimo dispositivo. L'effetto distorsivo che quest'ultima modalità di impiego del terminale potrebbe comportare è tuttavia ad oggi fortemente mitigato in virtù dell'incremento delle connessioni attraverso dispositivi mobili avutosi negli ultimi anni ed alla ormai assai capillare diffusione dei terminali di accesso ad internet fra la popolazione, da cui è derivato un rapporto pressoché biunivoco fra dispositivo e singolo utente. Proprio quest'ultimo aspetto, inerente le modalità d'uso dei dispositivi elettronici, porta dunque a poter condividere l'assunto secondo cui nella maggior parte dei casi la profilazione per fini commerciali comporta l'archiviazione nel terminale dell'utente di informazioni aventi il carattere di dati personali, in quanto inerenti al tracciamento dell'attività *on-line* di un soggetto identificato o identificabile.

Guardando alla regola di carattere generale di cui all'art. 5.3, parte prima, della direttiva 2002/58/CE, essa ammette due eccezioni, inerenti rispettivamente il caso in cui l'archiviazione tecnica o l'accesso siano realizzati « al solo fine » di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica oppure « nella misura strettamente necessaria » al fornitore di un servizio della società dell'informazione per erogare tale servizio quando esplicitamente richiesto dall'abbonato o dall'utente. In pratica le eccezioni concernono le mere funzionalità tecniche (es. i c.d. *load balancing session cookies*[30]) oppure ipotesi in cui si possa desumere una sorta di consenso implicito derivante dalla scelta di un determinato servizio la cui fruizione è strettamente connessa all'impiego dei *cookies* (es. i c.d. *shopping basket cookies*, *user-input cookies*, gli *authentication cookies* di sessione ed i *multimedia player session cookies*[31])[32].

Tralasciando tali ipotesi derogatorie, le modifiche introdotte con la direttiva 2009/136/CE mutano il modello relativo alle informazioni archiviate nei terminali degli utenti dall'originario *opt-out*[33] all'attuale *opt-in*[34], in maniera indubbiamente più coerente

[30] Cfr. Article 29 Data Protection Working Party, *Opinion 4/2012 on Cookie Consent Exemption*, cit., 8; sulla nozione di *cookie* cfr. invece Article 29 Data Protection Working Party, *Working Document. Privacy on the Internet — An integrated EU Approach to On-line Data Protection* —, adottato il 21 novembre 2000, secondo cui: « Cookies are pieces of data that can be stored in text files that may be put on the Internet user's hard disk, while a copy may be kept by the website. They are a standard part of HTTP traffic, and can as such be transported unobstructed with the IP-traffic ».

[31] Cfr. Article 29 Data Protection Working Party, *Opinion 4/2012 on Cookie Consent Exemption*, cit., 6 s.

[32] Per un'analisi specifica dei casi che non rientrano nelle eccezioni di cui *supra* nel testo, cfr. Article 29 Data Protection Working Party, *ult. op. cit.*, 9 ss. Va inoltre osservato come il disposto dell'art. 5.3 della direttiva 2002/58/CE abbia una portata di carattere generale che lo rende neutro rispetto alla tecnologia applicata e rilevante in relazione all'impiego di altre soluzioni di monitoraggio quali ad esempio gli *spyware* od i *malware*.

[33] L'art. 5.3 della direttiva 2002/58/CE prevedeva infatti che l'uso di reti di

con i principi generali definiti in materia dalla direttiva 95/46/CE[35], laddove infatti è quest'ultimo approccio ad essere stato prescelto.

Questo mutamento di prospettiva ha trovato le resistenze degli operatori del settore pubblicitario ed anche per tale ragione i vari stati hanno tardato nel dare attuazione alla direttiva, che sarebbe dovuta avvenire entro il 25 maggio 2011. A tale data solamente nove stati avevano infatti introdotto norme conformi al nuovo testo (Danimarca, Estonia, Finlandia, Irlanda, Lettonia, Malta, Svezia e Regno Unito). In sede di attuazione della direttiva, preso atto del passaggio al modello incentrato sull'*opt-in*, le *lobby* delle società di *advertising* hanno focalizzato la propria attenzione sul disposto del considerando n. 66 della direttiva 2009/136/CE, nella parte in cui afferma che, riguardo all'utilizzo di *cookies* e di tecnologie similari, « il consenso dell'utente al trattamento può essere espresso mediante l'uso delle opportune impostazioni di un motore di ricerca o di un'altra applicazione, qualora ciò si riveli tecnicamente fattibile ed efficace, conformemente alle pertinenti disposizioni della direttiva 95/46/CE ». In tal senso alcuni Paesi — quali il Regno Unito[36], l'Irlanda[37], la Francia[38], la Slovacchia[39] e la Spagna[40] — nell'attuare la direttiva hanno ravvisato nelle opzioni del *browser* definite dall'utente una valida manifestazione del consenso alla ricezione dei *cookies*.

Poiché rispetto al settaggio del *browser* con riguardo ai *cookies*, come con riguardo al DNT, si ripropone l'opzione fra accettazione di default (dei *cookies*) ovvero il rifiuto indiscriminato come regola di base, con conseguenze diametralmente opposte sulle possibilità di profilazione commerciale[41]. Ne consegue che gli operatori pubblicitari sono favorevoli a considerare il settaggio dei *browser* quali manifestazione di volontà dell'utente optando per l'accettazione dei *cookies* come regola di default. Tale possibile impostazione non pare tuttavia soddisfare le condizioni necessarie per consentire un legittimo trattamento dei dati acquisiti mediante

comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente fosse consentito solamente previa informativa ed a condizione che a quest'ultimo fosse « offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento ».

[34] Cfr. Article 29 Data Protection Working Party, *Parere 2/2010 sulla pubblicità comportamentale online*, cit., 12 s. ed Article 29 Data Protection Working Party, *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware*, adottata il 23 febbraio 1999, 3.

[35] Cfr. art. 7, direttiva 95/46/CE.

[36] Cfr. Statutory Instruments No. 1208 of 2011, in *http://www.legislation.gov.uk*.

[37] Cfr. Statutory Instruments No. 336 of 2011, in *http://dataprotection.ie*.

[38] Cfr. Ordonnance n. 2011-1012 du 24 août 2011 relative aux communications électroniques, Article 37.

[39] Cfr. art. 55 (5), regolamento 351/2011.

[40] Cfr. art. 22, ley 34/2002 dell'11 luglio 2002.

[41] Cfr. *supra* nota 21.

l'impiego dei *cookies*, poiché l'art. 5 della direttiva 2002/58/CE richiede che l'interessato « abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo » e la direttiva 95/46/CE, che costituisce il riferimento principale in materia[42], prevede che il consenso dell'interessato al trattamento debba essere, oltre che libero, specifico ed informato[43]. Ne consegue che l'utilizzo del browser senza mutare l'opzione di default volta ad accettare i *cokies* non è idonea a manifestare il consenso in quanto non chiarisce se il mantenimento di tale opzione derivi da una scelta consapevole o sia solo segno di indifferenza o inconsapevolezza[44]. A ciò si aggiunga che vengono altresì a mancare la specificità del consenso e la natura informata dello stesso rispetto al trattamento posto in essere attraverso l'impiego dei diversi *cookies* ricevuti[45].

Se dunque, in conformità al principio dell'*opt-in* adottato in generale dalla normativa comunitaria in materia di trattamento dati[46], pare doversi optare per il rifiuto dei *cookies* di default da parte del *browser*[47] occorre tuttavia rilevare come neppure nell'eventuale scelta successiva dell'utente di mutare i parametri del *browser* nel senso dell'indiscriminata accettazione di qualsiasi *cookies* possa ravvisarsi una valida manifestazione di volontà, venendo a mancare la specificità del consenso manifestato[48].

Alla luce delle considerazioni formulate si deve dunque concludere che una configurazione di *default* dei *browser* che escluda l'accettazione dei *cookies* unita ad un assenso manifestato caso per caso, sulla base delle informazioni previamente ricevute con riguardo alle modalità di trattamento dati correlate al singolo *cookies*, pare costituire la soluzione maggiormente conforme[49] alle indicazioni comunitarie[50]. Lo stesso considerando n. 66 della diret-

[42] Cfr. art. 1.2, direttiva 2002/58/CE.

[43] Cfr. art. 2, lett. *h*), direttiva 1995/46/CE.

[44] Cfr. Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, adottata il 13 luglio 2011, 32 e 35 s.: « consent based on the lack of individuals' action [...] does not meet the requirements of valid consent under the Directive 95/46/EC. The same conclusion applies to browser settings which would accept by default the targeting of the user (through the use of cookies) ». Cfr. altresì Article 29 Data Protection Working Party, *Parere 2/2010 sulla pubblicità comportamentale online*, cit., 15: « L'interessato medio non è consapevole del tracciamento del suo comportamento in rete né conosce le finalità del tracciamento, ecc. Non sempre è a conoscenza del modo in cui usare le impostazioni del browser per respingere i cookie, sebbene tali informazioni siano contenute nell'informativa sulla privacy. È erroneo ritenere che l'inattività dell'interessato (ovvero il fatto che questi non provveda a impostare il browser per respingere i cookie) fornisca una manifestazione chiara e univoca delle sue intenzioni ».

[45] Cfr. Article 29 Data Protection Working Party, *Parere 2/2010 sulla pubblicità comportamentale online*, cit., 16.

[46] Art. 5, direttiva 2002/58/CE.

[47] Cfr. Article 29 Data Protection Working Party, *Parere 2/2010 sulla pubblicità comportamentale online*, cit., 17.

[48] Cfr. Article 29 Data Protection Working Party, *op. ult. cit.*, 16.

[49] Rimane tuttavia la criticità correlata alla possibilità di individuare e trattare diversamente quei *cookies* che, ai sensi dell'art. 5.3, direttiva 2002/58/CE, non sono soggetti al previo consenso dell'interessato.

[50] Cfr. Commission nationale de l'in-

tiva 2009/136/CE non ravvisa nel settaggio dei *browser* una modalità di espressione del consenso comunque valida, bensì ne limita espressamente l'efficacia dichiarativa richiedendo che la soluzione adottata sia « tecnicamente [...] efficace » e risulti conforme alla direttiva 95/46/CE.

Per le ragioni espresse, considerando i diversi profili dell'informativa e dell'acquisizione del consenso, le soluzioni più efficaci in termini di chiarezza procedimentale sembrano essere quelle incentrate sulla « negoziazione » della ricezione dei *cookies* attraverso le pagine web dei singoli siti[51], ovviamente integrabili con le opzioni dei *browser*. Nello specifico al momento del primo accesso alla pagina web di un sito può comparire un *banner* ovvero una sovrimpressione contenenti l'informativa e la richiesta del consenso alla ricezione dei *cookies*[52].

Un processo decisionale non unitario ed onnicomprensivo, bensì casistico e destinato a ripetersi durante la navigazione *on-line* non deve tuttavia indurre a ritenere che in tal modo la normale fluida navigazione da una pagina all'altra del web si trasformerà in una sorta di corsa ad ostacoli. A tal proposito l'accettazione individualizzata dei *cookies* non implica necessariamente continue richieste di consenso al trattamento, poiché una volta accettato o rifiutato un determinato *cookie*, l'informazione sulla volontà dell'utente potrà essere memorizzata nel terminale di quest'ultimo, escludendo successive richieste[53]. Ove poi un sito web utilizzi una plu-

formatique et des libertés, *Ce que le « Paquet Télécom » change pour les cookies*, 26 aprile 2012, in *http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/ce-que-le-paquet-telecom-change-pour-les-cookies/*; cfr. anche Article 29 Data Protection Working Party, *Parere 2/2010 sulla pubblicità comportamentale online*, cit., 25 s., secondo cui « le impostazioni del browser sono idonee a trasmettere il consenso soltanto in circostanze assai limitate, in particolare quando il browser è impostato di default in modo tale da respingere tutti i cookie e l'utente ha modificato le impostazioni per accettare i *cookie* dopo essere stato pienamente informato del nome del responsabile del trattamento, delle finalità del trattamento e dei dati che vengono raccolti ».

[51] I soggetti coinvolti nella profilazione non sono infatti solamente i fornitori di reti pubblicitarie, bensì anche i gestori dei siti web che a tali reti aderiscono consentendo la tracciabilità degli utenti che visitano le loro pagine web, ne consegue che in capo a quest'ultimi, in ragione del loro rapporto di collaborazione con i fornitori, possano ricadere alcuni obblighi come quello di offrire un'adeguata informativa agli utenti circa l'impiego dei *cookies*. Cfr. in tal senso Article 29 Data Protection Working Party, *Parere 2/2010 sulla pubblicità comportamentale online*, cit., 12 s.

[52] Meno consigliabile è invece il ricorso alle finestre c.d. « pop-up », in quanto nei *browser* è possibile selezionare l'opzione che ne disabilita la visualizzazione durante la navigazione.

[53] Cfr. in tal senso la procedura indicata in Article 29 Data Protection Working Party, *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, cit., 10 s. Al fine di memorizzare la decisione occorrerà che sul terminale dell'utente venga installato un *cookie* positivo o negativo rispetto all'ipotesi specifica di profilazione ed ovviamente anche tale *cookie* che memorizza la volontà di rifiutare o di accettare i *cookies* dovrà essere preceduto da un'informativa e richiede il previo consenso, ai sensi dell'art. 5.3, direttiva 2002/58/CE. All'utente dovrà essere tuttavia riconosciuta anche la possibilità di rifiutare quest'ultima tipologia di *cookie* « di rifiuto », ma in

ralità di fornitori di servizi di tracciabilità sarà possibile aggregare in un'unica pagina o *banner* o sovrimpressione tutte le diverse opzioni, in maniera da evitare ripetute richieste[54].

Le informazioni inerenti la ricezione dei *cookies* potrebbero infine essere inserite nelle condizioni generali di contratto e si potrebbe considerare l'accettazione di quest'ultime come utile ai fini del consenso al trattamento. Rispetto a tale alternativa vanno formulate però due osservazioni.

In primo luogo la regola dell'*opt-in* di cui all'art. 5.3, direttiva 2002/58/CE, trova un'esplicita deroga nel caso in cui l'impiego dei *cookies* risulti « strettamente necessari[o] al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio », ne consegue che qualora venga rispettata tale condizione l'inserimento di previsioni *ad hoc* nelle condizioni generali di contratto è persino superflua. Secondariamente, qualora invece le condizioni del servizio *on-line* prevedano l'impiego di *cookies* ai fini della profilazione del fruitore del servizio senza che ciò sia « strettamente necessario » rispetto all'erogazione della prestazione, si deve ritenere che l'accettazione delle stesse non possa costituire una valida manifestazione di volontà con riguardo al trattamento dati[55]. In queste ipotesi infatti si richiede solitamente un'accettazione cumulativa di una pluralità di marcatori con finalità fra loro differenti, viene così a mancare la specificità del consenso prestato e, in molti casi, la puntualità dell'informativa con riguardo a ciascun singolo trattamento.

Da ultimo va considerata l'incidenza del trascorrere del tempo sulla volontà manifestata dall'utente rispetto alla profilazione mediante i *cookies*. A tal proposito il considerando n. 25 della direttiva 2002/58/CE afferma che « l'offerta di informazioni e del diritto di opporsi può essere fornita una sola volta per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione e applicarsi anche a tutti gli usi successivi, che possono essere fatti, di tali dispositivi durante successive connessioni », tuttavia, considerata la sensibilità dell'utente medio per questi temi, pare condivisibile sul punto l'interpretazione restrittiva data dall'Article 29 Data Protection Working Party, secondo cui occorre comunque delimitare la validità temporale del consenso prestato, fornire adeguate informazioni all'u-

tal caso, ove ritorni al sito in questione verrà nuovamente richiesto il suo consenso alla ricezione dei *cookies*, agendo diversamente invece non riceverà alcuna richiesta né verrà inviato alcun *cookie* volto al tracciamento, tanto dal singolo sito quanto da quelli consorziati utilizzanti il medesimo *cookie*.

[54] Cfr. Article 29 Data Protection Working Party, *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, cit., 11.

[55] Cfr. CNIL, *Ce que le « Paquet Télécom » change pour les cookies*, 26 aprile 2012, cit.

tente e renderlo edotto circa la possibilità di revocare in qualsiasi momento il consenso prestato[56].

2.2. (*segue*): LE NORME NAZIONALI DI ATTUAZIONE.

Rispetto all'articolato quadro costituito dalle disposizione comunitarie, dall'interpretazione delle stesse offerta dall'Article 29 Data Protection Working Party, nonché dalle esperienze straniere concernenti l'attuazione della direttiva 2009/136/CE, l'apporto e l'elaborazione del legislatore italiano e della nazionale data *protection authority* paiono piuttosto contenuti.

Occorre tuttavia rilevare come, sotto il profilo normativo, la legislazione italiana — nello specifico l'art. 122 D.Lgs. 196/2003[57] — fosse già orientata nel senso dell'*opt-in*, ed altresì in termini restrittivi, poiché, in difformità dall'art. 53 della direttiva 2002/58/CE nel suo testo originario, negava qualsiasi forma di tracciabilità attraverso *cookies* e simili, salvo demandare ad un codice deontologico — poi non venuto alla luce — la definizione delle ipotesi di deroga[58], limitate alla trasmissione delle comunicazioni ed alla fornitura di un servizio richiesto dall'interessato[59]. Ne consegue che l'attuazione della direttiva 2009/136/CE[60] ha di fatto ampliato

[56] Cfr. Article 29 Data Protection Working Party, *Parere 2/2010 sulla pubblicità comportamentale online*, cit., 18 s., ove altresì si « ritiene fondamentale » che i fornitori di reti pubblicitarie « elaborino modalità per informare periodicamente le persone del monitoraggio in corso ».

[57] Cfr. a riguardo A. Sica, *sub* Articoli 121-132, in *La nuova disciplina della privacy*, a cura di S. Sica-P. Stanzione, Bologna, 2005, 555 ss.

[58] Questo il testo dell'art. 122 D.Lgs. 196/2003 anteriormente alle modifiche apportate con il D.Lgs. 69/2012:

« 1. Salvo quanto previsto dal comma 2, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

2. Il codice di deontologia di cui all'articolo 133 individua i presupposti e i limiti entro i quali l'uso della rete nei modi di cui al comma 1, per determinati scopi legittimi relativi alla memorizzazione tecnica per il tempo strettamente necessario alla trasmissione della comunicazione o a fornire uno specifico servizio richiesto dall'abbonato a dall'utente, è consentito al fornitore del servizio di comunicazione elettronica nei riguardi dell'abbonato e dell'utente che abbiano espresso il consenso sulla base di una previa informativa ai sensi dell'articolo 13 che indichi analiticamente, in modo chiaro e preciso, le finalità e la durata del trattamento ». Cfr. a riguardo Gar., 10 maggio 2006, doc. web. 1298709.

[59] In quest'ultimi casi la legittimità del trattamento era inoltre subordinata alla previa acquisizione del consenso dell'interessato, quando invece la normativa comunitaria non lo prevedeva, cfr. art. 5.3, direttiva 2002/58/CE nella formulazione originaria.

[60] Questo il testo dell'art. 122 D.Lgs. 196/2003, a seguito delle modifiche introdotte con il D.Lgs. 69/2012:

« 1. L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con le modalità semplificate di cui all'articolo 13, comma 3. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o

l'impiego dei *cookies*, poiché il legislatore nel ricopiare il testo comunitario ha fatto venir meno il generale divieto all'utilizzo degli stessi al di fuori delle ipotesi di trasmissione delle comunicazioni o fornitura di un servizio richiesto dall'interessato, sostituendovi una generale autorizzazione all'impiego dei *cookies* con il previo consenso informato dell'interessato, relegando a norma di chiusura il testo originario dell'art. 122, comma 1, D.Lgs. 196/2003[61].

Più incerta è invece la posizione del legislatore italiano circa il possibile impiego delle impostazioni dei *browser* come modalità di espressione della volontà dell'interessato con riguardo al tracciamento, né dall'autorità garante sono ad oggi pervenuti chiarimenti interpretativi a tal proposito. Nello specifico, nel « recepire » le indicazioni provenienti dal considerando n. 66 della direttiva 2009/136/CE[62], non paiono essere state tenute in adeguato conto le osservazioni fromulate dall'Article 29 Data Protection Working Party illustrate nel precedente paragrafo. A ciò si aggiunga che, mentre nel dare attuazione al testo dell'art. 5.3, direttiva 2002/58/CE, come modificato dalla direttiva del 2009 da ultimo richiamata, il legislatore ha mantenuto inalterato il testo comunitario, nel trasporre il considerando n. 66 ha invece apportato alcune rilevanti modifiche che paiono mutarne il significato.

Mentre infatti, con riguardo ai mezzi impiegati, il considerando n. 66 prevede la possibilità di manifestare il consenso attraverso le impostazioni dei « browser or other applications », l'art. 122, comma 2, D.Lgs. 196/2003 novellato, in parziale difformità dalle indicazioni contenute nella legge delega[63], adotta un più generico riferimento ai « programmi informatici »[64] e, soprattutto, estende

dall'utente a erogare tale servizio. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente.

2. Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente.

2-*bis*. Salvo quanto previsto dal comma 1, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente ».

[61] Nel mutare la propria impostazione il legislatore ha poi ritenuto di introdurre la possibilità di informare l'utente avvalendosi delle modalità di cui all'art. 13, comma 3, D.Lgs. 196/2003, con il coinvolgimento degli *stakeholders* di riferimento. La scelta pare condivisibile, tenuto conto dell'esigenza di conciliare la completezza dell'informazione con la rapidità della navigazione *on-line*. La medesima soluzione è stata infatti adottata in situazione in cui si sono manifestate esigenze similari, cfr. Gar., Adempimenti semplificati per il customer care (inbound), 15 novembre 2007, doc. web n. 1462788.

[62] Cfr. considerando n. 66, direttiva 2009/136/CE.

[63] Cfr. art. 9, comma 4, lett. *i*), L. 15 dicembre 2011, n. 217, in cui si fa solo riferimento all'esigenza di informare l'utente « circa le modalità di espressione del proprio consenso, in particolare mediante le opzioni dei programmi per la navigazione nella rete internet o altre applicazioni ».

[64] Incidentalmente va rilevato come anche la versione in lingua italiana del con-

l'eccezione anche agli strumenti *hardware* (« dispositivi »). La variazione di maggior rilievo riguarda poi le condizioni di ammissibilità cui è soggetta tale diversa modalità di manifestazione del consenso: nel considerando n. 66 si richiede che il ricorso ai *browser* o ad altri applicativi per esprimere la volontà sia « technically possible and effective », mentre nel D.Lgs. 69/2012 si prevede che gli strumenti impiegati « siano di facile e chiara utilizzabilità per il contraente o l'utente ». Viene dunque a scomparire nel testo italiano la condizione generale rappresentata dall'efficacia della soluzione, intesa come idoneità ad esprimere la volontà del singolo, nulla prevedendo in proposito. Si aggiunge invece un elemento non presente nel considerando n. 66, quello dell'utilizzabilità dello strumento impiegato. Utilizzabilità ed efficacia non sono tuttavia concetti identici: la prima riguarda la semplicità di impiego di uno strumento, e nulla dice circa l'idoneità dello stesso a consentire una manifestazione indiretta della volontà dell'utilizzatore, mentre la seconda concerne il raggiungimento della finalità prefissata (manifestare la volontà attraverso un comportamento attivo) e non si cura della maggior o minor complessità con cui ciò avviene, sebbene la facilità d'uso possa costituire uno dei parametri utili per valutare la possibilità di raggiungere lo scopo.

Non è dato sapere perché il legislatore, così poco propenso a mutare il dettato degli articoli della direttiva nel darvi attuazione, abbia poi deciso di incidere sul testo di un considerando, tuttavia il risultato finale pare essere quello di un ampliamento interpretativo della deroga prevista dall'art. 5.3 direttiva 2002/58/CE, poco chiaro[65] e coerente con le indicazioni comunitarie.

La rilevanza delle norme in questione, correlata alle implicazioni sulle modalità di gestione dei siti web e soprattutto delle tecniche di *advertising*, avrebbe poi richiesto una maggior celerità nell'attuazione della direttiva e, soprattutto, un adeguato intervento di formazione e di controllo sulle prassi applicative. In tal senso l'esperienza italiana è assai lontana da quella del Regno Unito, ove si è tempestivamente dato attuazione alla direttiva, prevedendo però nel contempo un periodo di dodici mesi affinché le imprese e le altre organizzazioni avessero modo di implementare le soluzioni adeguate per conformare le proprie prassi alle nuove

siderando n. 66, direttiva 2009/136/CE, sia tutt'altro che felice, in quanto il termine « browser » è stato tradotto « motore di ricerca », confondendo i programmi funzionali alla navigazione *on-line* (es. Firefox, Microsoft Internet Explorer, Google Chrome, ecc.) con i servizi di ricerca ed indicizzazione di pagine web quali Google o Bing.

[65] Il generico riferimento alla possibilità di « utilizza[re] specifiche configurazioni di programmi informatici o di dispositivi » non scioglie infatti il nodo cruciale circa le modalità di impiego di tali sistemi affinché possano costituire valido strumento per l'espressione del consenso, non essendo specificato nulla circa la configurazione di *default* e le eventuali condizioni necessarie affinché il consenso possa essere manifestato attraverso la configurazione di tali programmi o dispositivi.

disposizioni riguardanti la profilazione[66], svolgendo nel contempo l'Information Commissioner's Office un ruolo di sensibilizzazione e formazione in materia[67].

3. Il valore delle informazioni e le esigenze di contrastare l'accesso illegittimo ai dati.

Se, come si è avuto modo di rilevare, le informazioni personali hanno da tempo acquisito una notevole importanza strategica ed economica e se, nel contempo, viene sempre più generalmente riconosciuto un coinvolgimento diretto dell'interessato nella circolazione di questa nuova merce immateriale, ne consegue che tanto il lavoro di raccolta ed elaborazione posto in essere da chi sfrutta le informazioni, quanto le garanzie poste a tutela dell'interessato incentrate sulla procedimentalizzazione della gestione e sul rispetto delle norme a protezione dei dati da parte degli autori del trattamento, possono risultare vanificate ove si realizzino degli accessi illegittimi ai dati cui conseguano eventuali impieghi illeciti di quest'ultimi.

In tema di sicurezza e di contrasto al crescente fenomeno dei furti di dati o alla più generale problematica delle criticità concernenti la sicurezza dei dati archiviati, vengono quindi a convergere sia le esigenze e gli interessi delle imprese e, più in generale, di chi sfrutta le informazioni per le proprie finalità commerciali e non, sia quelle dei singoli interessati dal trattamento che rischiano di vedere vanificate le garanzie fornite da un'adeguata informativa e dall'acquisizione di un consenso liberamente espresso.

Non è dunque un caso che il problema dei c.d. *data breaches*, risulti essere al centro dell'attenzione dei regolatori, a prescindere dalle impostazioni di fondo e dalle valenze ideologiche con cui si avvicinano alla regolamentazione dei dati personali. Tanto la legislazione comunitaria[68], quanto la regolamentazione in materia di

[66] Cfr. il provvedimento Information Commissioner's Office (ICO), *Enforcing the revised Privacy and Electronic Communications Regulations (PECR)*, maggio 2012, in *http://www.ico.gov.uk*. In questo documento, in cui l'ICO chiarisce in che modo intende vigilare sull'attuazione delle nuove disposizioni, si riconosce che « in many cases, implementation of the rule requiring consent for cookies will be challenging for organisations » e che un'immediata attuazione delle stesse « could though significantly restrict the operation of internet services that users generally take for granted ». Sulla base di tali presupposti l'ICO conclude che « will though allow a lead in period of 12 months for organisations to develop ways of meeting the cookie related requirements of the 2011 Regulations before he will move towards the approach set out in his Data Protection Regulatory Action Policy and consider using his enforcement powers to compel them to do so in appropriate cases. This lead in period will end in May 2012 ».

[67] Cfr. i materiali informativi disponibili all'indirizzo: *http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx*.

[68] Si vedano in proposito gli artt. 31 e 32 della recente proposta di Regolamento

consumer data privacy in corso di elaborazione negli USA[69], quanto quelle asiatiche[70], prendono infatti esplicitamente in considerazione questo aspetto, su cui paiono inoltre convergere le soluzioni avanzate, in ragione della marcata connotazione tecnica del problema e della comunemente avvertita rilevanza economica (e politica) del contrasto delle vulnerabilità dei sistemi di archiviazione di dati.

Rispetto all'attuale scenario globale che, coerentemente con la crescita dei flussi informativi e della loro rilevanza, sembra volgere verso una maggior protezione rispetto agli eventi pregiudizievoli per la conservazione dei dati, l'Unione Europea con la direttiva 2009/136/CE, modificando l'art. 4 della direttiva 2002/58/CE, già aveva predisposto le prime indicazioni nel senso di un incremento della tutela di dati[71], limitando tuttavia l'intervento in materia di *data breach* ai soli fornitori di un servizio di comunicazione elettronica accessibile al pubblico, anziché prevederlo quale criterio generale come invece è accaduto negli attuali progetti di riforma elaborati sia a livello comunitario che nei Paesi terzi.

Il D.Lgs. 69/2012 recepisce ora *in toto* le indicazioni della direttiva 2002/58/CE definendo le modalità di notifica dei casi di violazione della sicurezza dei dati[72], integrando il capo I del titolo V del D.Lgs. 196/2003, laddove sono previste le disposizioni in materia di misure di sicurezza dei dati personali[73]. Coerentemente con i

---

comunitario in materia di tutela dei dati personali, cfr. European Commission, *Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final, Brussels, 25 gennaio 2012, in *http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm*.

69 Cfr. il documento del Governo statunitense *Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, febbraio 2012, 39 e 48, in *http://www.whitehouse.gov*. Già 47 stati, il District of Columbia e vari territori statunitensi hanno adottate normative locali in materia di *data breach notification*, manca tuttavia ad oggi un quadro regolamentare uniforme a cui invece mira il documento governativo.

70 Si vedano la legge sudcoreana sulla *data protection* dell'11 marzo 2011 e la legge taiwanese di riforma della normativa nazionale in materia di protezione dei dati personali del 26 maggio 2010 (in vigore dal 2012), su quest'ultima cfr. G. Greenleaf, *Taiwan Revises its Data Protection Act*, in *Privacy Laws & Business International Report*, Nos. 108 & 109, 2010-2011, disponibile *on-line* in *http://papers.ssrn.com*.

71 Si vedano a tal riguardo le linee guida definite dall'European Network and Information Security Agency (ENISA), cfr. Enisa, *Data breach notifications in the EU*, 2011, in *http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn*.

72 Ai sensi dell'art. 4, comma 3, lett. *g-bis*), introdotta dal D.Lgs. 69/2012, per « violazione di dati personali » si deve intendere una « violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico ». Cfr. art. 2, lett. *i*), direttiva 2002/58/CE.

73 Va in proposito rilevato come, limitatamente al settore creditizio il Garante per la protezione dei dati personali avesse già previsto, ai sensi dell'art. 154, comma 1, lett. *c*), D.Lgs. 196/2003 l'obbligo di comunicare senza ritardo agli interessati « le operazioni di trattamento illecito effettuate — sui dati personali allo stesso riferiti —

nuovi obblighi sono state inoltre introdotte sanzioni *ad hoc*, come richiesto dalle disposizioni comunitarie[74].

Nello specifico le norme introdotte mirano a realizzare gli obiettivi di tutela rispetto al *data breach* mediante un intervento che si articola in quattro direzioni: la parziale riformulazione delle misure di sicurezza che i fornitori di un servizio di comunicazione elettronica accessibile al pubblico sono tenuti ad adottare, la previsione a carico degli stessi di specifici obblighi di comunicazione, l'obbligo di conservare un inventario delle violazioni di dati personali, l'attribuzione al Garante di congrui poteri di vigilanza e sanzionatori.

Poche sono state le modifiche apportate all'art. 32, D.Lgs. 196/2003, con riguardo alle misure di sicurezza. L'aspetto di maggior rilievo concerne l'acquisizione da parte del legislatore della consapevolezza circa la complessità funzionale dei servizi in questione e della conseguente necessità di coinvolgere nell'attuazione delle misure di sicurezza anche i soggetti che si interpongono a diversi livelli nell'erogazione degli stessi[75]. Nella medesima ottica è stato previsto il coinvolgimento di quest'ultimi soggetti anche con riguardo agli adempimenti conseguenti ad una violazione di dati personali introdotti con il nuovo art. 32-*bis* del Codice in materia di protezione dei dati personali[76].

Merita inoltre di essere sottolineato il richiamo all'attuazione di una « politica di sicurezza » ad opera dei fornitori, aspetto su cui in via interpretativa l'autorità garante potrebbe intervenire auspicabilmente invertendo la tendenza in atto, orientata ad una limitata attenzione per questi profili, manifestatasi in provvedimenti quali l'eliminazione dell'obbligo di redigere il documento programmatico sulla sicurezza[77] e che va in senso opposto rispetto

dagli incaricati », nonché di comunicare « tempestivamente al Garante — fornendo gli opportuni dettagli — i casi in cui risultino accertate violazioni, accidentali o illecite, nella protezione dei dati personali, purché di particolare rilevanza per la qualità o la quantità di dati coinvolti e/o il numero di clienti interessati, dalle quali derivino la distruzione, la perdita, la modifica, la rivelazione non autorizzata dei dati della clientela ». Cfr. Gar., Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie, 12 maggio 2011, doc. *web* n. 1813953, punti 5.1. e 5.2.

74 Cfr. art. 4.4, direttiva 2002/58/CE.

75 Nella nuova formulazione dell'art. 32, comma 1, D.Lgs. 196/2003 si prevede infatti che il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotti le misure di sicurezza sia all'interno della propria organizzazione, sia « attraverso altri soggetti a cui sia affidata l'erogazione del [...] servizio ». Cfr. a riguardo anche ENISA, *Data breach notifications in the EU*, cit., 25.

76 Cfr. art. 32-*bis*, comma 8, D.Lgs. 196/2003, ai sensi del quale ove il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ne affidi l'erogazione a terzi, gli affidatari « sono tenuti a comunicare al fornitore senza indebito ritardo tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti di cui al presente articolo ».

77 Cfr. D.L. 9 febbraio 2012, n. 5, convertito con modificazioni dalla L. 4 aprile 2012, n. 35, che ha abrogato l'art. 32, comma 1, lett. *g*) e l'art. 1-*bis*, D.Lgs. 196/2003, nonché i punti da 19 a 19.8 ed il punto 26 dell'Allegato B al D.Lgs. 196/2003.

agli orientamenti comunitari ispirati alla *privacy by design* ed al *privacy impact assessment*.

Con riguardo alle misure *ex post* da porre in essere in seguito alla violazione di dati personali, ruolo centrale è attribuito alla comunicazione al Garante e, ove prevista, agli interessati dell'avvenuta violazione. La comunicazione al Garante[78], come anche l'ulteriore obbligo di conservare un inventario delle violazioni[79], sono finalizzate ad agevolare le funzioni di monitoraggio e controllo, avendo a disposizione dati il più possibile completi circa gli incidenti di sicurezza[80]. Con riguardo invece alla comunicazione rivolta agli interessati, essa si rende necessaria ogni qualvolta la violazione possa arrecare loro pregiudizio sia rispetto alla tutela dei dati personali che della riservatezza[81], posto che in tali casi le conseguenze negative possono essere molteplici e significative sia sul piano economico che reputazionale, identitario e morale[82]. Ne consegue che, rispetto ai soggetti interessati, non sarà sufficiente la semplice comunicazione dell'avvenuta violazione della sicurezza, bensì occorrerà anche rendere edotti quest'ultimi circa le misure opportune onde limitare gli eventuali effetti pregiudizievoli e le modalità con cui ottenere maggiori informazioni sull'accaduto[83]. Stante il presupposto della natura potenzialmente pregiudizievole della violazione, la comunicazione agli interessati non sarà dovuta allorquando, in ragione delle modalità tecniche adottate nella gestione dei dati da parte del fornitore, detto pregiudizio non possa verificarsi[84].

Al fine di garantire un efficace *enforcement* di tali disposizioni il legislatore ha inoltre previsto l'attribuzione di compiti specifici in

---

78 Cfr. art. 32-*bis*, commi 1 e 5, D.Lgs. 196/2003.

79 Cfr. art. 32-*bis*, comma 7, D.Lgs. 196/2003.

80 Cfr. considerando n. 58, direttiva 2009/136/CE.

81 Cfr. art. 32-*bis*, comma 2, D.Lgs. 196/2003; ai sensi del successivo comma 4, « ove il fornitore non vi abbia già provveduto, il Garante può, considerate le presumibili ripercussioni negative della violazione, obbligare lo stesso a comunicare al contraente o ad altra persona l'avvenuta violazione. ».

82 Cfr. considerando n. 61, direttiva 2009/136/CE.

83 Cfr. art. 32-*bis*, commi 4, 5, e 6, D.Lgs. 196/2003; cfr. altresì considerando n. 59, direttiva 2009/136/CE.

84 In tal senso l'art. 32-*bis*, comma 3, D.Lgs. 196/2003 prevede che la comunicazione di cui al comma 2 non sia dovuta ove il fornitore abbia dimostrato al Garante di aver impiegato misure tecnologiche di protezione « che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione ». Cfr. a riguardo Gar., Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali, 26 luglio 2012, doc. web n. 1915485, punto 7.1, ove viene inoltre data un'interpretazione estensiva del potere riconosciuto dall'art. 32-*bis*, comma 4, D.Lgs. 196/2003, in virtù del quale « ove il fornitore non vi abbia già provveduto, il Garante può, considerate le presumibili ripercussioni negative della violazione, obbligare lo stesso a comunicare al contraente o ad altra persona l'avvenuta violazione ». Nello specifico l'autorità garante ritiene infatti che « tale possibilità prescinde dal fatto che il fornitore abbia reso inintelligibili i dati violati: tale evenienza riduce, non fa venir meno, il rischio che i dati violati siano comunque decifrabili e che, pertanto, il Garante imponga di effettuare comunque la comunicazione ».

materia in capo al Garante[85], nonché individuato apposite sanzioni per le ipotesi di violazione di ciascuno degli obblighi introdotti[86].

Ai sensi dell'art. 32-*bis*, comma 6, D.Lgs. 196/2003, sono state poi da ultimo definite le linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali ad opera del Garante[87], recanti alcune specifiche in merito alle modalità di analisi dei rischi[88] e di comunicazione delle violazioni dei dati personali. Proprio con riguardo a quest'ultimo aspetto, in particolare le comunicazioni rivolte ai soggetti interessati dalle violazioni, l'interpretazione data proposta dal Garante[89] appare controversa in merito alle ipotesi in cui la comunicazione dell'avvenuta violazione dei dati personali agli interessati non sarebbe necessaria in quanto relativa ad una violazione inidonea a « rischia[re] di arrecare pregiudizio ai dati personali o alla riservatezza di contraente o di altra persona » ai sensi dell'art. 32-*bis*, comma 2, D.Lgs. 196/2003. Non paiono in specie convincenti criteri discretivi incentrati sulla natura dei dati (sensibili o meno), sulla quantità dei dati inerenti l'interessato o sull'« attualità » degli stessi[90], potendo derivare un danno all'interessato anche dall'accesso illegittimo a dati comuni, quantitativamente limitati e non aggiornati[91]. A tal proposito occorre inoltre interrogarsi sull'opportunità, sull'affidabilità e sulla realizzabilità della definizione di metriche uniformi capaci di definire *ex ante* l'incidenza della violazione dei dati in termini di pregiudizio arrecati al sin-

[85] Cfr. art. 32-*bis*, commi 3, 4, 6 e 7, D.Lgs. 196/2003.

[86] Cfr. art. 162-*ter* D.Lgs. 196/2003 introdotto dal D.Lgs. 69/2012 e le modifiche da quest'ultimo apportate ai successivi artt. 164-*bis*, comma 1, e 168, comma 1. In particolare nei casi di omessa o tardiva comunicazione agli interessati dell'avvenuta violazione dei dati personali è prevista una sanzione amministrativa da centocinquanta euro a mille euro « per ciascun contraente o altra persona nei cui confronti venga omessa o ritardata la comunicazione », senza applicazione dell'art. 8 l 24 novembre 1981, n. 689, fino ad un massimo del 5% del volume d'affari realizzato dal fornitore del servizio nell'ultimo esercizio, fatta salva la possibilità di aumentare la sanzione fino al quadruplo quando possa risultare inefficace in ragione delle condizioni economiche del contravventore, ai sensi dell'art. 164-*bis*, comma 4.

[87] Cfr. Gar., Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali, 26 luglio 2012, doc. web n. 1915485, v. anche il « Modello destinato ai fornitori di servizi di comunicazione elettronica per la comunicazione dei casi di violazione dei dati personali (data breach) », in *http://www.garanteprivacy.it/garante/document?ID=1915835*.

[88] Cfr. in specie il punto 4.1 delle citate linee guida.

[89] Cfr. Gar., Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali, 26 luglio 2012, doc. web n. 1915485, punto 7.3.

[90] Nel provvedimento citato alla precedente nota, l'« attualità » viene intesa dal Garante come « il tempo trascorso dall'acquisizione dei dati stessi e dal loro inserimento nei database del fornitore ».

[91] Con riguardo al rapporto fra « attualità » del dato e pregiudizio, va anzi rilevato come, sotto il profilo reputazionale, in taluni casi l'eventuale divulgazione di un dato non recente possa arrecare maggior pregiudizio di quanto non accada con un dato aggiornato, potendo generare una falsa rappresentazione dell'identità del soggetto.

golo, piuttosto che porre in essere un'analisi dei rischi caso per caso *ex post*[92].

[92] Un'indagine condotta a riguardo dall'ENISA ha rilevato come nel settore privato « most [operators] agree, however, that it is important to rate incidents according to a specific threat level. Few operators indicated that they had a specific methodology or procedure for determining risk level. In most cases, the process takes place on an ad hoc basis »; cfr. ENISA, *Data breach notifications in the EU*, cit., 25.