IAIC MiBACT DGBIC CREDA

Diritto Mercato Tecnologia

10 Gennaio 2017

Considerazioni in tema di rapporto tra sviluppo del *mobile payment* e tutela della *privacy* degli utenti

Marina Romano

Nuova Editrice Universitaria

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.
2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.
3. L'identità del valutatore è coperta da anonimato.
4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088855, fax 06.8070483, www.iaic.it, info@iaic.it

Considerazioni in tema di rapporto tra sviluppo del *mobile payment* e tutela della *privacy* degli utenti

Marina Romano
Università degli Studi di Napoli Parthenope

Abstract: Negli ultimi anni, il progresso delle tecnologie informatiche ha portato, nell'ambito delle transazioni di denaro, applicazioni sempre più nuove, come è avvenuto con l'introduzione del sistema del *mobile payment* che consente di effettuare pagamenti o trasferimenti di denaro attraverso il telefono mobile nella duplice modalità del *proximity* o del *remote*. Ciò, se da una parte ha determinato una semplificazione, un risparmio di tempi e di costi ed un passo in avanti nel contrasto dell'evasione fiscale, dall'altra, è diventato una minaccia alla tutela della *privacy* per gli utenti.

In recent years, the advancement of computer technology has increasingly brought about the creation of new applications in the field of money transactions, including the introduction of the mobile payment system that allows payments or transfers of money through the mobile phone both in the proximity and remote modes. This, on the one hand, has led to simplification, time and cost savings and a step forward in contrasting tax evasion; on the other hand, has become a threat to the users' privacy.

1. Il sistema di *mobile payment*

Gran parte dei beni e dei servizi viene oggi acquistata o utilizzata dagli utenti attraverso la tecnologia informatica che consente di avere una serie di van-

taggi sia in termini di risparmio, che di ottimizzazione del tempo. Le nuove tecnologie sono, a loro volta, in continua evoluzione ed offrono ai clienti modalità di erogazione attraverso la rete informatica sempre nuove ed articolate.

Pietra miliare di questa tendenza è stata l'introduzione del servizio di *mobile payment*, ovvero la possibilità di effettuare pagamenti o trasferimenti di denaro tramite telefono mobile, che molti fornitori, che solitamente erogavano servizi di comunicazione tradizionali, hanno negli ultimi anni implementato per offrire sempre più ampie opportunità sul mercato[1]. Si può affermare che la diffusione del *mobile payment* ha, difatti, radicalmente modificato il settore del commercio tradizionale ed elettronico[2], determinando un'accelerazione nella conclusione delle transazioni commerciali ed un'accentuazione dei processi di smaterializzazione dei trasferimenti di denaro[3]. Benchè il *mobile payment* possa effettuarsi attraverso due modalità (*proximity* e *remote*), il consumatore identifica questo sistema di pagamento come la possibilità di effettuare qualsiasi tipo di pagamento tramite *smartphone* o altri dispositivi mobili.

Tecnicamente, il pagamento del bene o del servizio acquistato avviene o mediante carte di credito, attraverso una disposizione che viene inviata per il tramite del telefono avvicinando il dispositivo mobile dotato di tecnologia NFC (*Near Field Communication*) che fornisce connettività *wireless* bidirezionale a corto raggio ad un apposito lettore POS posto presso il punto vendita dell'esercente da cui si acquista il bene (c.d. acquisto con modalità *proximity*), oppure con addebito e conseguente decurtazione del costo dal credito telefonico, per i clienti dotati di una carta ricaricabile, oppure ancora con addebito sul conto telefonico, per i clienti in abbonamento (c.d. acquisto con modalità *remote)*. In quest'ultimo caso, i dati di pagamento dei clienti sono aggiunti a quelli del loro traffico telefonico.

---

[1] S. Moneti, *"*Mobile payments*": gli sviluppi del mercato e l'inquadramento normativo*, in *Analisi giuridica dell'economia*, 2015, p. 101 ss.; M. Cucchiani; M. Ravasio, *Lo sviluppo del* Mobile Payment *in Italia; i vantaggi per i consumatori e gli ostacoli al suo decollo*, in *Micro & Macro Marketing*, 2011, p. 641 ss.

[2] A. Fratini; F. Poggi, *Il quadro regolamentare delle comunicazioni elettroniche: analisi dei mercati* wholesale *della telefonia mobile*, in *Contratto e impresa Europa*, 2006, p. 263 ss.

[3] A. Longo, *Il cellulare alla conquista dei sistemi*, in *www.archiviostorico.ilsole24ore.com,* 2016.

Questo sistema di pagamenti consente anzitutto una notevole semplificazione, in quanto agevola le transazioni e la sicurezza del buon fine delle stesse attraverso una radicale esclusione del denaro contante. Consente, altresì, un notevole risparmio di costi che, viceversa, sarebbe necessario sostenere per la gestione di grandi masse di denaro contante; nonché costituisce un ulteriore passo in avanti nel combattere l'evasione fiscale.

Occorre tuttavia che un progresso di tale portata non si ripercuota negativamente su altri traguardi già conquistati e considerati altrettanto fondamentali nella vita dei soggetti - utenti - quali il diritto alla *privacy*. È difatti preoccupazione diffusa che l'efficienza e la sicurezza del sistema dei pagamenti debba procedere di pari passo con un'adeguata protezione delle informazioni degli utenti/consumatori.

2. Il profilo della tutela della *privacy* degli utenti che utilizzano il *mobile payment*

Il Garante per il trattamento dei dati personali, nella sua relazione annuale al Governo sull'attività svolta nel 2015, ha evidenziato come sia fondamentale promuovere una maggiore consapevolezza sui rischi intrinseci della tecnologia sotto il profilo della tutela dell'autonomia e delle libertà degli individui. Ha difatti sottolineato che l'elemento secondo cui l'economia è attualmente fondata sui dati, comporta che poche grandi aziende, che hanno accesso ad essi, hanno il potere di profilazione dei consumi e delle preferenze dei soggetti a livello mondiale e su questo fondano il costante accumulo della loro ricchezza[4].

La tecnologia insidia quindi la concreta possibilità di tutela della *privacy* e con essa la stessa libertà delle persone. L'ultimo decennio, sotto questo profilo, è stato infatti caratterizzato da una crescente affermazione del *web* al prezzo di una diminuzione della tutela della identità delle persone.

[4] Cfr. l'intervista al Garante della *Privacy*, *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2867069*.

Le informazioni, come è noto, costituiscono un bene, un valore; le informazioni che riguardano i dati personali, in particolare, sono un bene molto prezioso perché in grado di orientare il mercato mondiale dei consumi[5]. È dunque necessario essere in grado di adottare meccanismi idonei a garantire che le potenzialità del *web* non siano sfruttate a scapito della riservatezza e quindi della tutela dei diritti fondamentali dei soggetti.

In tema di protezione dei dati personali ed in particolare delle implicazioni tra *web* e circolazione dei dati personali in rete, la dottrina ha messo in luce alcuni profili di criticità proprio in riferimento all'esigenza della tutela degli utenti[6].

L'art. 1 del d.lgs. 30 giugno 2003 n. 196, il codice in materia di protezione dei dati personali o Codice Privacy[7], ha sancito il principio secondo il quale «chiunque ha diritto alla protezione dei dati personali». Vi è però da dire che si è determinato negli ultimi anni un significativo avanzamento tecnologico nei processi di comunicazione in rete a cui non è seguito un altrettanto rapido adeguamento della normativa esistente, con la conseguenza che l'obiettivo di assicurare un appropriato livello di protezione dei dati personali, come stabilito dal Codice della Privacy, non sempre è stato raggiunto[8].

---

[5] In argomento: E. C. Pallone, *La profilazione degli individui connessi a* internet*:* privacy on line *e valore economico dei dati personali*, in *Ciberspazio e dir.*, 2015, p. 295 ss.; M. Soffientini, *Trattamento dei dati personali – Profilazione* on line*: nuove regole*, in *Dir. prat. lav.*, 2015, p. 1545 ss.; A. Toma, *Big data, bigger profilings and bigger market solutions: privacy like "little thumb"*?, *http://www.altalex.com/index.php?idstr=24&indnot=68916*, in *www.altalex.com*, 2014.

[6] Seppure da un'angolazione diversa, è stato rilevato che «deve essere consentito alla persona, a tutela della sua identità, di esercitare il proprio diritto di libertà informatica, che consiste nel poter disporre dei propri dati», così, testualmente: M. F. Cocuccio, *Il diritto all'identità personale e l'identità "digitale"*, in *Dir. fam.*, 2016, p. 952. Cfr. anche: G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, in *Dir. Informaz.*, 2015, p. 779 ss.; D. Vanni, *Protezione dei dati personali (Diritto civile)*, *Aggiornamento* 2013, in *Dig. Civ*., Torino, p. 535; G. Ferraro, Apps *dei cellulari: e la* privacy*?*, in *www.ilquotidianogiuridico.it*, 2011.

[7] Per un primo commento al Codice della Privacy: C. M. Nanna, *Accesso ai dati personali e tutela dei diritti fondamentali nel sistema del d.lgs. 196/2003*, nota a *Cass., 9 gennaio 2013, n. 349*, in *Corriere giur*., 2013, p. 1546 ss.; A. Del Ninno, *La tutela dei dati personali- Guida pratica al codice della privacy (d.leg. 30 giugno 2003 n. 196)*, Padova, 2006.

[8] In tema di rapporto tra sviluppo della rete e tutela della *privacy* i contributi sono numerosi; tra tanti, cfr.: A. M. Gambino, Open data *e* data protection *nel* cloud computing, in *Riv. elet-*

Ad esempio, nel giro di pochi anni siamo passati dal *WEB 1.0*, rappresentato da siti informativi c.d. statici che non offrivano la possibilità di interagire con altri utenti, ma consentivano essenzialmente l'accesso a motori di ricerca, al *WEB 2.0*, nel quale la rete offre a chiunque la possibilità di partecipare alla creazione ed alla condivisione di contenuti digitali.

Ciò è stato possibile grazie a diverse infrastrutture, piattaforme ed altre applicazioni *software* che hanno consentito una condivisione potremmo dire globale di musica, di foto, di filmati, di testi, di opinioni ecc. In questa nuova dimensione, ciascuno è allo stesso tempo fruitore e produttore di contenuti. Ciò ha posto un problema in termini di circolazione dei dati personali e dunque di tutela della persona, soprattutto in conseguenza dell'utilizzo nei diversi *social network* dei tasti "di apprezzamento e di condivisione"[9].

Questi tasti hanno un'utilità per i *provider* che in tal modo riescono a convogliare il traffico verso i propri siti *web* con ricadute positive in termini di pubblicità; per i membri dei *social network* sono invece uno strumento per aggiungere informazioni circa i propri interessi sulle pagine dei loro profili personali.

Con tale sistema è possibile che siano comunicati dagli utenti dati relativi alle loro convinzioni religiose, filosofiche, alle opinioni politiche, all'adesione a partiti, sindacati o anche ad associazioni od organizzazioni costituite ai fini più disparati, sino a comunicare quelli relativi allo stato di salute ed alla vita sessuale.

In effetti, il rischio è proprio connesso alla semplicità del meccanismo che richiede, dal punto di vista dell'utente, che per partecipare alla vita sul *social network* basti attivare un semplice *click* senza contestualmente cogliere a pieno le conseguenze di tale rapido gesto. In altre parole "si condivide

---

tronica dir., econ., management, 2014, p. 77 ss.; M. Carta, *Diritto alla vita privata ed* Internet *nell'esperienza giuridica europea e internazionale*, in *Dir. Informaz.*, 2014, p. 1 ss.; M. Soffientini, Cloud computing *e* privacy, in *Dir. prat. lav*., 2013, p. 2465 ss.; P. Galdieri, *Il trattamento illecito del dato nei* social networks, in *Giur. mer.*, 2012, p. 2697 ss.; F. Prosperi*, Tecnologia informatica e tutela della* privacy, in *Corti Marchigiane*, 2006, p. 3 ss.; V. Cuffaro, *Uso e abuso dei dati personali nelle comunicazioni elettroniche*, in *Corr. merito*, 2006, p. 1385 ss.; M. Fortino Silvestri, *Il soggetto privato di fronte alle "nuove" tecnologie: alcuni aspetti problematici*, in *Riv. dir. cost.,* 2005, p. 97.

[9] G. De Luca, Privacy *e* social networks, *http://www.altalex.com/index.php?idstr=24&idnot=11674*, in *www.altalex.com*, 2010.

senza riflettere", fornendo inconsapevolmente e contestualmente dati strettamente personali, talvolta anche dati sensibili.

Questa modalità, come già anticipato, si traduce in un vantaggio del *social network site* in quanto la sua attività è pianificata appositamente per gestire queste informazioni volte anche a profilare e a catalogare i fruitori del servizio in funzione del massimo sfruttamento commerciale attraverso la pubblicità[10]. Ciò ha condotto ad un ripensamento dello stesso concetto di *privacy* che sembrerebbe attualmente assumere il significato di diritto a mantenere il controllo sulle proprie informazioni, oppure a dominare la circolazione del flusso di informazioni personali che insieme costituiscono l'identità dell'individuo, la sua posizione sociale, o anche quello che è stato definito il suo corpo elettronico[11].

È possibile dunque rilevare come lo sviluppo della tecnologia e la nuova era del *WEB 2.0* abbia già mostrato alcune criticità rispetto a quanto stabilito nel d.lgs. 2003/196, in particolar modo in riferimento alle regole in tema di dati sensibili, cioè ai dati che riguardano la personalità etico-sociale dell'individuo e le sue caratteristiche psico-sanitarie.

In proposito, l'elencazione delle fattispecie di dati sensibili contenuta nell'art. 4 codice *privacy* ha natura tassativa e non esemplificativa, in quanto dati sottoposti ad una rigida disciplina di tutela. L'elenco dei dati sensibili è dunque chiuso; è stato tuttavia rilevato che l'espressione contenuta nell'art. 4

[10] In argomento, per tutti: S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p. 47 ss. L'A. ha evidenziato che è proprio questo il vantaggio che il fornitore del servizio trae poiché quando l'utente accede al servizio e spunta una casella che rimanda alle condizioni generali di utilizzo, ivi comprese le condizioni che riguardano la *privacy*, accetta che i propri dati vengano trattati per le finalità ivi descritte. I dati per cui si consente il trattamento sono sia quelli forniti dallo stesso utente al momento della registrazione, sia quelli raccolti successivamente sulla base della navigazione svolta in *Internet* dall'utente stesso (ad esempio, i siti visitati, le interazioni con altri utenti, le caratteristiche tecniche del dispositivo utilizzato per accedere a *Internet*).
Cfr.: A. Palmieri, Marketing *diretto: indicazioni per la tutela della* privacy *dei destinatari dei messaggi promozionali*, nota a *Cass., 24 giugno 2014, n. 14326*, in *Foro it*., 2014, I, c. 2453.

[11] Cfr.: AA.VV, *Libera circolazione e protezione dei dati personali*, in Panetta (a cura di), Milano, 2006, Vol. I e II; S. Niger, *Le nuove dimensioni della* privacy*: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

«idonei a rivelare» consenta una certa elasticità[12] nel senso specifico che non si escluderebbero altri dati che potrebbero avere un collegamento anche solo potenziale con dati sensibili della persona[13], come ad esempio lo stato di salute o le convinzioni religiose.

Il trattamento dei dati sensibili è soggetto infatti a norme più rigorose rispetto al trattamento dei dati personali, in quanto il danno derivante da una loro utilizzazione illecita è più grave per la persona rispetto a quello derivante dalla utilizzazione di altri dati.

Regola di carattere generale è che se il trattamento dei dati sensibili è effettuato da un soggetto privato, come nel caso dei *social network*, è previsto che il consenso dell'interessato debba essere dato in forma scritta e debba essere documentato. Si tratta di forma *ad substantiam* e può trattarsi anche di firma elettronica.

Sulla base di queste premesse, anche per il *mobile payment* si pone l'esigenza di un'adeguata protezione dei dati personali, atteso che attraverso questo meccanismo molte informazioni che riguardano l'utente vengono conosciute dagli operatori del servizio.

3. Il quadro normativo di riferimento.

Per la disciplina in tema di *mobile payment* occorre far riferimento anzitutto al d.l. 27 gennaio 2010 n. 11[14] che ha recepito la dir. 2007/64/CE relativa ai servizi di pagamento nel mercato interno, ovvero la c.d. PSD1 (*Payment Services Directive*). La portata innovativa della PSD1 è stata individuata nell'aver aperto il mercato dei servizi di pagamento anche ad operatori

[12] A.R. Popoli, Social network *e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Dir. Informaz.,* 2014, p. 981 ss.; L. Coppola, *Il dato personale è sensibile quando è idoneo a rivelare una situazione di debolezza o di disagio dell'individuo: una scelta discutibile della Corte di Cassazione*, nota a *Cass., 22 settembre 2011, n. 19365*, in *Corr. giur.*, 2012, p. 934 ss.

[13] G. Finocchiaro, Privacy *e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, p. 57 ss.

[14] Per un primo commento al d.l. 11/2010: M. Onza, *La "trasparenza" dei "servizi di pagamento" in Italia (un itinerario conoscitivo)*, in *Banca borsa tit. cred*., 2013, p. 577 ss.

c.d. non bancari, con l'obiettivo di armonizzare il quadro giuridico di riferimento in vista del regolare funzionamento del sistema dei pagamenti e di assicurare efficienza e sicurezza per tutti i soggetti coinvolti in queste operazioni[15].

Il significato di questa apertura costituisce anzitutto una presa d'atto dei nuovi traguardi tecnologici che consentono che i pagamenti - trasferimenti di denaro - vengano effettuati attraverso la rete digitale od informatica anche da soggetti diversi da quelli bancari.

In primo luogo, l'art. 2 della dir., trasfuso nell'art. 1, comma 1, lett.b) del d.lgs. 11/2010, definisce il c.d. *positive scope* ovvero l'indicazione del tipo di attività che rientra nell'ambito della disciplina dei servizi di pagamento. Esso riguarda l'attività degli operatori delle reti di comunicazione digitali o informatiche che agiscono quali intermediari tra l'utente del servizio di pagamento, effettuato con un dispositivo di telecomunicazione digitale o informatico, ed il fornitore dei beni e dei servizi richiesti da quell'utente. Per questi soggetti non bancari, ammessi quindi a pieno titolo nel sistema dei pagamenti all'interno dell'UE, la direttiva in esame prevede un regime semplificato rispetto a quello degli istituti bancari tradizionali ed una preventiva autorizzazione da parte delle Autorità competenti.

Al *positive scope* si contrappone il c.d. *negative scope*, ovvero il perimetro delle esclusioni dalle prescrizioni stabilite per i soggetti intermediari non bancari di cui sopra. Specificamente, l'art. 3, lett. l), della dir., trasfuso nell'art. 2, comma 2, d.lgs. 11/2010, stabilisce che nelle esclusioni rientrano le operazioni di pagamento, eseguite sempre con un dispositivo di telecomunicazione digitale o informatico, relative all'acquisto di beni e servizi digitali consegnati o utilizzati attraverso il dispositivo gestito dall'operatore di telecomunicazione digitale o informatica *che svolga anche altre funzioni.*

A tale esclusione si riferisce il *considerando* n. 6 della dir., il quale ha chiarito che, qualora l'attività dell'operatore non si esaurisca con la semplice intermediazione di pagamento, si determina una fattispecie in cui l'operatore "aggiunge un qualcosa" alla semplice fruizione del bene o del servizio digi-

[15] In tal senso il «Provvedimento di attuazione del Titolo II del Decreto Legislativo n. 11 del 27 gennaio 2010 relativo ai sevizi di pagamento (Diritti ed obblighi delle parti)» emanato dalla Banca d'Italia il 5 luglio 2011.

tale, e questo qualcosa può consistere in funzioni di accesso, di distribuzione o consultazione.

La contrapposizione tra attività rientranti nel *positive scope* e attività rientranti nel *negative scope* corrisponde in sostanza alla contrapposizione tra la figura dell'operatore non bancario che agisce come *mero* intermediario del servizio di pagamento e la figura dell'operatore non bancario che, *oltre* all'intermediazione, *offre anche* altre funzioni, quali l'accesso, la ricerca e la distribuzione, in modo tale che senza tali funzioni non sarebbe possibile per l'utente fruire di quel bene o servizio con le medesime modalità.

La dir. ha dunque aperto il mercato dei servizi di pagamento anche ad operatori non bancari ma ha, al contempo, inteso "esonerare" il mercato dei micropagamenti dall'osservanza di regole più stringenti dettate per le operazioni di pagamento, alla condizione che l'attività posta in essere dall'operatore comprenda anche altre funzioni che incidono in modo pregnante sulle modalità di fruizione di quel bene o di quel servizio.

L'elencazione riportata nel *considerando* n. 6 della dir. non può, peraltro, reputarsi tassativa atteso che la stessa Banca d'Italia, nel Provvedimento del 5 luglio 2011 in tema di «Attuazione del Titolo II del decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti)», ha chiarito che un esempio di esclusione è rappresentato dai pagamenti effettuati all'operatore della rete di telecomunicazioni relativi all'acquisto di contenuti multimediali che possono essere scaricati sul telefono cellulare o su altro dispositivo, come *smartphone*, *decoder*, *tablet* o *PC*, nell'ambito dei servizi di trasmissione dati offerti dallo spesso operatore[16].

Per quanto riguarda specificamente le condizioni dell'esclusione, esse sono state individuate anzitutto nella necessità che le operazioni di pagamento siano riferibili all'acquisto di beni o servizi digitali.

In secondo luogo, che l'operatore di telecomunicazione non agisca quale *mero* intermediario dell'operazione di pagamento, ma la sua attività sia più estesa, ovvero comprensiva di altri servizi che, come già evidenziato, caratterizzano nella sostanza le modalità di fruizione del bene o servizio da parte dell'acquirente.

[16] Cfr. nota 9 del Provvedimento della Banca d'Italia del 5 luglio 2011 *cit*.

Infine, che la consegna o l'utilizzo dei beni o servizi in questione siano effettuati tramite il dispositivo di telecomunicazione digitale o informatico gestito dallo stesso operatore[17].

In ordine alla questione cruciale dell'eventuale violazione dei dati personali[18], il Garante della *privacy*, nel Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni dei c.d. *data breaches* del 4 aprile 2013, pubblicato sulla GU n. 97 del 26/4/2013, ha menzionato espressamente l'ipotesi in cui il fornitore di servizi di comunicazione elettronica accessibili al pubblico possa anche offrire il servizio di *mobile payment* per includerla nell'ambito degli obblighi ed adempimenti in materia di «violazione dei dati personali».

Più specificamente, la materia delle violazioni dei dati personali è disciplinata dall'art. 4 della dir. 2002/58/CE, c.d. direttiva *e-Privacy*, modificata dalla dir. 2009/136/CE, nonché dal d.lgs. 28 maggio 2012 n. 69 con il quale tali dir. sono state recepite nel nostro ordinamento. Quest'ultimo aveva già apportato diverse modifiche ed alcune integrazioni al Codice Privacy[19].

In particolare, erano state introdotte modifiche alle definizioni dell'art. 4 in tema di *chiamate*, *reti di comunicazione elettronica*, *rete pubblica di comunicazioni,* adeguandole a quelle già presenti nell'ordinamento comunitario.

Era stata, inoltre, introdotta nel Codice della Privacy una nuova definizione di violazione, ovvero quella di «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», mediante l'aggiunta della lettera g-*bis* al comma 2 dell'art. 4.

Un'altra modifica era stata quella dell'art. 32 Codice Privacy sugli obblighi di sicurezza per i fornitori di servizi di comunicazione elettronica acces-

[17] Cfr. il Provvedimento della Banca d'Italia del 5 luglio 2011 *cit*., par. 2.2.9.

[18] In argomento, cfr.: A. Montelero, *Si rafforza la tutela dei dati personali:* data breach notification *e limiti alla profilazione mediante i* cookies, in *Dir. Informaz.*, 2012, p. 781 ss.; E. Pellecchia, *La responsabilità civile per trattamento dei dati personali*, in *Resp. civ. prev.*, 2006, p. 221 ss.

[19] G. Busia, *Commento al D.Lgs. 28 maggio 2012 n. 69*, in *Guida al dir*., 2012, fasc. 27, p. 16.

sibili al pubblico, che erano stati estesi anche ai diversi soggetti cui è stata affidata l'erogazione dei predetti servizi.

Era stato infine aggiunto l'art. 32 *bis* in tema di «Adempimenti conseguenti ad una violazione di dati personali», che prevede misure che includono l'obbligo per un fornitore dei servizi di comunicazione elettronica di segnalare al Garante l'avvenuta violazione di dati personali e, qualora la violazione possa interessare dati o la riservatezza di un'altra persona, è prescritta la comunicazione della violazione anche a quest'ultima.

In proposito, i fornitori dei servizi di comunicazione elettronica sono obbligati, *ex* art. 132 *bis* Codice Privacy, ad istituire apposite e specifiche procedure interne per far fronte alle richieste di accesso ai propri dati personali inoltrate dagli utenti, nonché a fornire al Garante le informazioni su tali procedure, sul numero di richieste ricevute, sulle questioni di diritto sollevate e sulle risposte date.

In questo contesto normativo si è quindi inserito il Provvedimento del Garante del 4 aprile 2013 suindicato con cui sono state fornite le linee guida operative ed i modelli e *format* ufficiali per le notifiche dei casi di *data breach*.

Questi nuovi adempimenti gravano su quei soggetti che mettono a disposizione del pubblico servizi consistenti nella trasmissione di segnali su reti di comunicazioni elettroniche (art. 4, comma 2, lett. d) ed e) Codice Privacy, e per quanto specificamente riguarda il *mobile payment*, il Garante ha chiarito che i dati di pagamento dei clienti sono strettamente connessi a quelli di traffico telefonico degli stessi e pertanto, in caso di violazione di dati riguardanti tali servizi, il fornitore è tenuto agli obblighi di notifica.

Di conseguenza, la fattispecie del *mobile payment* è soggetta anche al Reg. UE 611/2013 emanato dalla Commissione il 24 giugno 2013 sulle misure in tema di violazioni di dati personali.

Tale atto ha adottato le misure tecniche di attuazione degli obblighi previsti dalla dir. 2002/58/CE relativamente agli *standard*, alle procedure ed ai *format* di comunicazione allo scopo di uniformare le procedure di comunicazione delle violazioni per i fornitori che operano su base transfrontaliera.

Sotto questo profilo, si può rilevare che il Reg. non contiene elementi di novità rispetto al Provvedimento del Garante del 4 aprile 2013 che è stato piuttosto dettagliato, avendo previsto anche i termini temporali – di 24 ore o

di tre giorni a seconda dei casi – entro i quali si deve procedere con le notifiche delle violazioni.

Gli elementi di novità del Reg. in ordine agli obblighi di notifica di *personal data breach* sono, invece, da ravvisarsi nella previsione secondo la quale il fornitore è tenuto ad informare il Garante di tutte le violazioni di dati personali senza poter decidere diversamente.

Inoltre, il Reg. ha stabilito che, se si verificano violazioni che rischiano di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona interessata, scatta l'obbligo di comunicare l'avvenuta violazione anche a questa persona e ne ha codificato i casi violazione.

L'art. 3, infatti, dispone che l'eventualità che una violazione di dati personali possa pregiudicare un abbonato o un'altra persona è valutata dai fornitori tenendo conto di alcune circostanze quali la natura ed il contenuto dei dati personali interessati quando, ad esempio, riguardino informazioni finanziarie, dati sensibili, dati biometrici (caratteristiche fisiche dell'individuo come le impronte digitali, le caratteristiche del viso ecc.) *file* di connessione ad *internet*, cronologie di navigazione in rete, elenchi delle chiamate, nonché quando la violazione possa comportare furto di identità o danni alla reputazione.

Altro elemento di novità del Reg. è stato il divieto ai fornitori di sfruttare l'obbligo di notifica al contraente od ad altra persona a scopo di *marketing*.

Infine il Reg., attraverso i suoi due allegati, ha stabilito il contenuto obbligatorio della notifica di violazione dei dati personali che il fornitore dei servizi di comunicazione elettronica deve trasmettere al Garante, nonché il contenuto della comunicazione che il fornitore dei servizi di comunicazione elettronica deve trasmettere al contraente o ad altre persone i cui dati personali sono stati interessati dalla violazione.

4. L'intervento dell'Autorità Garante della *privacy* in tema di *mobile payment*

In riferimento alla dir. del 2007, il Garante ha successivamente emanato il Provvedimento n. 3161560 del 22 maggio 2014, pubblicato sulla GU del 16 giugno 2014 n. 137.

Con questo provvedimento il Garante ha emanato le misure che devono essere adottate in relazione all'esigenza di un corretto utilizzo dei dati personali degli utenti che si avvalgono di servizi di pagamento o trasferimento di denaro tramite telefono cellulare, ovvero il *mobile payment*.

Nel provvedimento il Garante ha preso atto dell'enorme passo in avanti che è stato compiuto con questo sistema nel settore dei micropagamenti rispetto all'uso del contante, in particolar modo con riferimento all'obiettivo del risparmio di costi, ma viene evidenziato che, attraverso questo sistema, l'utente per poter accedere a questi nuovi servizi di pagamento deve fornire una serie di informazioni di carattere identificativo, che vanno dal numero di telefono, ai dati anagrafici, alle caratteristiche del prodotto richiesto e dell'importo speso, alla data ed all'ora dell'acquisto. In alcuni casi possono essere coinvolti anche dati di natura sensibile.

Viene quindi esplicitato l'obiettivo del provvedimento, ovvero far sì che il trattamento si svolga nel rispetto di quanto sancito nell'art. 11 del Codice Privacy, ovvero secondo i principi generali di liceità, pertinenza e non eccedenza, di correttezza e buona fede. Con questo obiettivo, il Garante individua una serie di puntuali prescrizioni dirette ai soggetti coinvolti nelle operazioni di *mobile payment* allo scopo di prevenire i rischi connessi ad un utilizzo improprio dei dati personali degli utenti[20].

Nel perseguimento di questo obiettivo, il Provvedimento in esame distingue quanti e quali sono i soggetti coinvolti, nonché viene specificato il ruolo da ciascuno di essi svolto[21] nell'operazione.

Tra essi, il primo è l'*operatore*, ovvero il fornitore di reti e servizi di comunicazione elettronica accessibili al pubblico attraverso cui offre all'utente il servizio di pagamento tramite telefono cellulare per l'acquisto di contenuti digitali (*mobile remote payment*) con due modalità. La prima consiste nell'addebito e la conseguente decurtazione del costo del bene a contenuto digitale acquistato dal credito telefonico, in caso di utenti in possesso di una

[20] Testualmente il Garante chiarisce che lo scopo del Provvedimento è quello di «garantire, in un mercato dei pagamenti sempre più dinamico, un uso sicuro e al contempo efficace delle informazioni che riguardano gli utenti», cfr. par. 2.

[21] Il Garante si esprime, a tal proposito, nei termini di un'architettura tecnico-organizzativa di riferimento nella comprensione del fenomeno, cfr. par. 2.

carta telefonica ricaricabile. La seconda riguarda gli utenti che abbiano sottoscritto in precedenza un contratto di abbonamento con l'operatore di riferimento, per cui il costo verrà addebitato direttamente sul conto telefonico.

Un altro soggetto è l'*aggregatore*, ovvero quel soggetto che mette a disposizione la piattaforma o interfaccia tecnologica, attraverso la quale l'utente può fruire del bene o servizio acquistato e ne cura la gestione. Il *merchant* è invece il fornitore dei contenuti digitali offerti, e l'utente o cliente è il titolare della USIM prepagata o postpagata.

Per poter utilizzare questo sistema di pagamento, il cliente deve fornire una serie di informazioni che vanno dai dati anagrafici, al numero del proprio telefonino, ai dati relativi al tipo di servizio o del prodotto digitale richiesto, ai dati relativi alla fatturazione, all'indirizzo di posta elettronica, all'indirizzo IP, sino a dati di natura sensibile *ex* art. 4, comma1, lett. d), Codice Privacy che possono essere desunti proprio dal contenuto del bene digitale richiesto.

Emerge, dunque, con evidenza il profilo della esigenza di tutela delle libertà fondamentali del soggetto che nel provvedimento del Garante viene declinata in una serie di misure, tra le quali un ruolo centrale assumono gli obblighi di informazione[22] preventiva che incombono indistintamente sull'operatore, sull'aggregatore e sul *merchant*.

L'informativa deve essere circostanziata, ovvero chiara e completa, e deve riguardare le finalità di erogazione del servizio. Deve specificare se i dati personali dell'utente sono trattati per scopi ulteriori, come ad esempio ricerche di mercato, *marketing* o invio di materiale pubblicitario o comunque di comunicazione dei dati a terzi[23]. In tutti questi ultimi casi, nell'informativa deve risultare con chiarezza che tali attività possono essere effettuate solo previo consenso[24] dell'utente per ciascuna finalità[25].

---

[22] In argomento: G. De Luca, *Informativa* privacy web*: non chiamatela "formalità"*, *http:/www.diritto.it/docs/31848*, in *www.diritto.it*, 2011.

[23] In proposito, si consideri che dal 1° ottobre 2016 è entrato in vigore il Codice deontologico per il trattamento dei dati personali effettuato ai fini di un'informazione commerciale, introdotto con delibera del Garante della *privacy* n. 479/2015, pubblicata sulla G.U. del 13 ottobre 2015.

[24] Sul consenso al trattamento dei dati, cfr.: S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in

Deve, altresì, risultare la menzione del soggetto designato responsabile del procedimento *ex* art. 29 Codice Privacy, nonché dell'esercizio da parte dell'utente dei diritti di accesso ai dati e di opposizione, secondo quanto stabilito dall'art. 7 Codice Privacy.

L'informativa deve infine riguardare gli eventuali dati sensibili e le relative modalità del loro trattamento, rispetto ai quali il consenso dell'interessato deve essere dato con modalità informatiche equiparabili allo scritto.

L'informativa va rilasciata al momento dell'iscrizione o adesione ai servizi fruibili tramite dispositivo mobile, ed è fornita secondo una modalità c.d. *layered* o a strati, resa necessaria considerando le dimensioni piuttosto contenute degli schermi dei terminali solitamente utilizzati in questo genere di operazioni.

Tale modalità si articola in più livelli. Un primo livello, relativo ad una prima informativa breve che appare in un'apposita sezione della pagina *web* dell'operatore o dell'aggregatore, ed è relativa agli elementi essenziali; segue quindi un'informativa più lunga e dettagliata alla quale si accede attraverso uno specifico *link*.

In tutti i casi in cui questo è necessario, l'utente presta il suo consenso attraverso un *flag* presente in un'apposita sezione della pagina *web* dell'operatore, oppure con altre idonee modalità informatiche.

Specifiche indicazioni sono poi previste per le operazioni di trasferimento dei dati tra i vari soggetti coinvolti nell'operazione allo scopo di evitare che essi possano venire a conoscenza di informazioni relative all'utente che esulano dalla specifica finalità della loro attività. È così previsto che il *merchant* debba classificare i servizi offerti secondo tabelle merceologiche generiche e solo dopo trasmetterle all'operatore il quale, a sua volta, deve usare tabelle

---

Europa dir. priv., 2016, p. 513 ss.; S. Niger*, Il "mito" del consenso alla luce del codice in materia di protezione dei dati personali*, in *Ciberspazio e dir*., 2005, p. 499 ss.

[25] In proposito, il Garante si rifà alla sua posizione espressa nel precedente Provvedimento del 28 maggio 1997, che può ritenersi consolidata, in base alla quale «il consenso può essere ritenuto effettivamente libero solo se si presenta come manifestazione del diritto all'autodeterminazione informativa, e dunque al riparo da qualsiasi pressione» e dunque l'utente deve essere destinatario di una specifica comunicazione nella quale sia indicato se il trattamento dei dati è relativo solo al servizio richiesto o anche ad ulteriori attività, in relazione alle quali il consenso deve essere prestato separatamente, per l'appunto per ciascuna attività, e in maniera specifica.

interne di classificazione basate sul genere di prodotti e non sul contenuto specifico di esse[26].

Il meccanismo di pagamento secondo il sistema *mobile* implica che l'operatore, che gestisce il numero di telefono dell'utente, debba verificare la sussistenza del credito telefonico e quindi inviare un messaggio al *merchant* che, tuttavia, deve limitarsi solo alla comunicazione dell'esito dell'operazione, senza che sia possibile risalire ad altre cause ostative inerenti l'utente, quali ad esempio l'insufficienza del credito telefonico[27].

Altre misure di cautela nel trattamento dei dati da parte dell'operatore riguardano la codifica di essi nell'ambito della propria organizzazione interna, nel senso di dover procedere ad una forma di "mascheramento dei dati", onde evitare il rischio di conoscenza da parte di qualsivoglia soggetto, anche addetto dell'operatore stesso.

È difatti previsto che gli addetti possano accedere ai dati solo per le operazioni di assistenza richiesta dagli utenti, ed in ogni caso solo dopo esser stati sottoposti ad una specifica procedura di autenticazione, c.d. forte, che ne consenta successivamente la tracciabilità e l'identificazione di colui che ha curato l'intervento di assistenza.

Altro aspetto è quello della profilazione dell'utenza che può scaturire dalla possibilità di correlare dati relativi a servizi diversi (ad esempio TV interattiva e telefono cellulare) riferiti allo stesso utente. Per evitare questo rischio si richiede che siano predisposti sistemi interni di rotazione attraverso i quali allo stesso utente sono applicate chiavi di codifica diverse.

Quando il contenuto dei servizi digitali è destinato ad un pubblico adulto, l'operatore deve poi prevedere misure di sicurezza adeguate che possono consistere nell'associazione a quel cliente di un PIN dispositivo per quel determinato prodotto.

I dati trattati possono essere conservati per un periodo di tempo limitato (sei mesi), alla scadenza del quale, in assenza di contestazioni, si deve pro-

[26] Nel caso invece di servizi in abbonamento, l'operatore può conoscere il nome del servizio acquistato dal cliente proprio per poter eseguire correttamente eventuali richieste di disattivazioni, od altro, che lo stesso cliente gli potrebbe richiede.

[27] Può essere solo inviato un *sms* all'utente con il quale l'operatore gli comunica le cause del mancato buon esito dell'operazione, tra cui anche quella dell'insufficienza del credito.

cedere alla cancellazione di essi dal proprio sistema. In proposito è prevista un'eccezione per l'indirizzo IP (ovvero di un codice numero che identifica un dispositivo collegato ad *internet*) che dovrà essere cancellato dal venditore al termine della transazione.

Inoltre, nel periodo di conservazione, l'accesso ai dati dovrà essere garantito tramite sistemi di "autenticazione forte" da parte del personale addetto e attraverso procedure di tracciamento degli accessi e delle operazioni effettuate.

Specifiche misure di cautela sono previste per gli aggregatori nella loro attività di reportistica indirizzata sia agli operatori, che ai *merchant* anche ai fini degli adempimenti di fatturazione o del pagamento delle *royalties.* Tali *report* non possono mai contenere riferimenti allo specifico contenuto del servizio richiesto dall'utente, ma sempre al genere di prodotto.

Dall'analisi del Provvedimento del Garante si evince che è stato stabilito che le misure a tutela della *privacy* dovranno essere adottate da tutti i soggetti coinvolti nella fornitura del servizio di micropagamento attraverso un dispositivo mobile, ovvero dagli operatori di comunicazione elettronica (ovvero le compagnie telefoniche che forniscono il servizio di pagamento tramite cellulare), gli aggregatori (ovvero le società che forniscono l'interfaccia tecnologica), i venditori (le aziende che offrono contenuti digitali e servizi), nonché ogni altro soggetto eventualmente coinvolto nella transazione (come quelli che consentono, anche tramite apposite *app*, l'accesso al mercato digitale).

Il termine entro il quale le misure adottate dal Garante avrebbero dovuto essere realizzate era stato previsto per il 15 dicembre 2014, ma su richiesta degli stessi operatori, il Garante, con Provvedimento n. 546 del 20 novembre 2014, lo ha prorogato al 31 marzo 2015.

5. La direttiva UE/2015/2366

Il 25 novembre 2015 è stata emanata la dir. 2015/ 2366 relativa ai servizi di pagamento nel mercato interno[28], di modifica delle dir. 2002/65 e

[28] Per un primo commento della dir., seppure da altre angolazioni: A. Blandini, *Servizi finanziari per via telematica e le prospettive del diritto societario* on line, in *Banca borsa tit. cred*., 2016, p. 46 ss.

2009/36. Essa abroga la dir. 2007/64 la PSD1 e dovrà essere recepita dal legislatore interno entro il 13 gennaio 2018.

La PSD2, come è stata subito etichettata, influenzerà lo sviluppo dei sistemi di pagamento elettronico nei prossimi anni ponendosi nella direzione di una maggiore tutela del consumatore, di un aumento dei servizi ed una maggiore apertura alla concorrenza.

In particolare la PSD2 interviene sia nel c.d. *positive scope*, ovvero l'ambito oggettivo di applicazione delle nuove regole, proponendo la definizione di nuovi servizi e la ridefinizione di altri già previsti dall'attuale PSD1, sia in quello del c.d. *negative scope*, ovvero il perimetro delle deroghe.

In riferimento alle dir. PSD1 e PSD2 il significato è dunque che nel *negative scope* si delinea il perimetro delle deroghe, ovvero l'indicazione di quelle attività relative ai servizi di pagamento che è possibile svolgere senza l'obbligo di operare nel regime di vigilanza previsto per gli intermediari di pagamento.

Ciò significa che un'attività rientrante nel *negative scope*, non è riservata ai PSP (Prestatori di Servizi di Pagamento), e pertanto, un soggetto non bancario può esercitarne il servizio senza operare come PSP, ossia senza l'obbligo di essere (o diventare) Istituto di Pagamento o IMEL (Istituti di moneta elettronica), nonché senza l'obbligo di ricorrere a soluzioni di partenariato con PSP autorizzati (Banche, Poste, Istituti di Pagamento, IMEL).

Per comprendere a pieno la direzione in cui si muove la dir. 2015/2366 occorre partire dall'analisi dei *considerando*. Specificamente, nel *considerando* n. 15, il legislatore comunitario chiarisce che il perimetro delle deroghe, che era stato stabilito nella dir. 2007/64 aveva lo scopo di incentivare lo sviluppo di nuovi modelli commerciali basati sulla vendita a basso costo di contenuti digitali e di servizi a tecnologia vocale. Tuttavia, tale perimetro delle esclusioni era stato formulato ambiguamente e pertanto l'esclusione è stata applicata in maniera disomogenea dai diversi SM, determinando mancanza di certezza giuridica sia per gli operatori, che per i consumatori.

Dalle informazioni provenienti dal mercato, il legislatore comunitario precisa altresì che i consumatori, pur volendo ricorrere a tale forma di transazione per i pagamenti di piccola entità, non lo hanno fatto in modo generalizzato così come era auspicabile.

Inoltre gli operatori spesso hanno sfruttato tale ambiguità nella formulazione e si sono talvolta considerati compresi nell'esclusione in modo illimitato.

Pertanto con la nuova dir. il legislatore si propone di chiarire l'ambiguità e di restringere il perimetro delle deroghe.

Anzitutto nella nuova PSD2, e precisamente nell'allegato 1, è stato eliminato quanto è attualmente presente nell'allegato alla PSD1 al punto 7 che dettaglia il *positive scope* stabilendo che sono soggetti all'ambito di applicazione della dir. 2007/64 «gli operatori del sistema o della rete di telecomunicazioni o digitale o informatica che agiscono esclusivamente come intermediario tra l'utente ed il fornitore».

La portata di questo cambiamento va letta alla luce del nuovo perimetro delle deroghe contenuto nell'art. 3 della nuova dir. alla lettera l, ovvero il nuovo *negative scope*, dove si stabilisce che l'esclusione dovrà riguardare i micropagamenti per i contenuti digitali e i servizi a tecnologia vocale, che il servizio di pagamento deve essere «in aggiunta» all'attività primaria dell'operatore, ed infine che il valore di ogni singola operazione non deve superare il limite di euro 50 ed il valore complessivo delle operazioni mensili non deve superare euro 300.

In altre parole, è stata ribadita sia la natura "ancillare" del servizio di pagamento nell'ambito dell'attività primaria dell'operatore, sia il riferimento al carattere digitale del contenuto della transazione. È stato però inserito esplicitamente il valore delle operazioni che possono godere dell'esclusione dall'ambito di applicazione della nuova direttiva.

L'intento del legislatore comunitario sembra, dunque, quello di voler incentivare al massimo la diffusione di un sistema di micropagamenti[29] per quanto concerne i beni di natura digitale e ciò pare confermato anche dalla

[29] Cfr.: E. Netti, *Nuovo slancio alla moneta digitale*, in *www.archiviostorico.ilsole24ore.com*, 2016; Id., *Il borsellino digitale da 164 miliardi*, in *www.archiviostorico.ilsole24ore.com*, 2016. In futuro si prevede, difatti, un' utilizzazione capillare dei micropagamenti attraverso il sistema *mobile*. Si considerino già i progressi che stanno avendo i trasferimenti di denaro tra privati con la piattaforma *Jiffy*, destinata ad aggredire il mercato dei micropagamenti. Si stima che a breve il sistema *Jiffy* permetterà di ricevere sul cellulare l'avviso di scadenza di un importo dovuto alla PA e di pagare in tempo reale con la *app* della propria banca.

espressa inclusione nell'ambito delle deroghe del c.d. mobile *ticketing*[30] e delle donazioni. Nel contempo, sono assicurate una serie dettagliata di misure a salvaguardia sia della trasparenza delle operazioni, che della sicurezza, della riservatezza e dell'integrità delle credenziali degli utenti.

Ciò è in linea con la necessità che l'accelerazione dei *mobile payments* sia accompagnata da un'adeguata tutela della *privacy* dei soggetti coinvolti nelle operazioni[31] ed è proprio in questa direzione che il legislatore nazionale, in occasione del recepimento della dir. dovrà operare con determinazione, anche alla luce del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 sulla *Privacy*, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati personali nell'Unione[32], destinato ad incidere in modo significativo sulla tutela della *privacy*.

---

[30] Sul *mobile ticketing*, il Garante per la protezione dei dati personali ha emanato uno Schema di provvedimento generale il 10 settembre 2015 n. 467 nel quale ha stabilito, tra l'altro, di avviare una procedura di consultazione pubblica, invitando tutti i soggetti interessati a far pervenire le proprie osservazioni. Nello schema di provvedimento viene anzitutto chiarito che tutte le misure indicate nei provvedimenti in tema di *mobile remote payment* devono essere osservate anche in questo settore. A questo complesso di regole se ne devono però aggiungere altre in ragione della specificità della fornitura del servizio di *mobile ticketing.*

[31] A tal proposito, sembrano significativi i risultati di un'indagine sulla *IOT (Internet of Things*), resa nota a settembre 2016 e svolta dalle Autorità Garanti della *Privacy* di 26 paesi per il *Privacy Sweep* 2016 appartenenti al *Global Privacy Enforcement Network* (GPEN) di cui fa parte anche il Garante italiano. L'indagine è stata condotta sulla *IOT*, ovvero un settore in crescente espansione che riguarda l'offerta di dispositivi elettronici connessi ad *internet*, come orologi, elettrodomestici e braccialetti intelligenti per il controllo del sonno o dell'indice glicemico, contatori elettronici e termostati di ultima generazione e le stesse automobili connesse ad *internet*. Da tale indagine è emerso che gli operatori del settore, che offrono questi beni e servizi, non sembrano aver sinora posto sufficiente attenzione all'aspetto della protezione dei dati personali. Non è stata riscontrata, infatti, un'adeguata attenzione al fatto che, oltre al nome ed al cognome dell'utente, anche il consumo elettrico di una persona o i suoi parametri vitali sono dati da proteggere. L'indagine si chiude quindi con un impegno da parte dei Garanti a monitorare che la crescita di questo settore di mercato non avvenga a danno della riservatezza dei dati personali degli utenti.
In argomento, cfr. anche: M. Soffientini, *Il futuro della* privacy*: dall'*internet of things *ai* big data, in *Dir. prat. lav.*, 2015, p. 809 ss.

[32] La data di entrata in vigore del suddetto reg. è fissata il 25 maggio 2018. Il nuovo reg. è destinato a riscrivere l'intera disciplina della *privacy* a livello europeo con l'obiettivo

di assicurare un'applicazione coerente ed omogenea delle norme sul trattamento dei dati personali. Per quanto riguarda il trattamento dei dati personali, gli SM dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle disposizioni contenute nel reg.

Le novità introdotte sono numerose; tra le tante, ed in specifico riferimento al tema del *mobile payment*, due avranno probabilmente una diretta applicazione. La prima consiste nell'aver previsto una nuova figura che si affianca a quelle tradizionali del *titolare*, del *responsabile* e dell'*incaricato* del trattamento, ovvero il *DPO* (*Data Protection Officer*) - Responsabile della protezione dei dati -, deputato a sorvegliare tutte le operazioni ove i trattamenti presentino specifici rischi. L'altra novità è l'introduzione dell'obbligo di tenere un «registro delle attività di trattamento», nonché quello di effettuare una «valutazione di impatto sulla protezione dei dati».

Diritto Mercato Tecnologia

Numeri Speciali

2016 Lo Statuto Etico Giuridico dei Campioni Biologici Umani
a cura di Dario Farace

La rivista "Diritto Mercato Tecnologia" intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall'interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.