Il Garante privacy ha adottato il provvedimento (doc. web n. 3161560) che disciplina il trattamento dei dati personali di chi usufruisce dei cosiddetti servizi di mobile remote payment, utilizzando *smartphone, tablet, pc*, stabilendo un primo quadro organico di regole in grado di assicurare la protezione dei dati senza penalizzare lo sviluppo del mercato digitale.

di Valentina FREDIANI

LE NUOVE REGOLE DEL GARANTE DELLA PRIVACY PER I PAGAMENTI CON *SMARTPHONE* E *TABLET*

Valentina FREDIANI *è avvocato e titolare dell'omonimo Studio che si occupa esclusivamente di diritto delle nuove tecnologie: Diritto informatico, Privacy, Conservazione e archiviazione sostitutiva, DL 231, Videosorveglianza, Contrattualistica, proprietà intellettuale, ecc.. È socio di AIPSI (Associazione Italiana Professionisti della Sicurezza Informatica); membro del Comitato Scientifico nonché Socio onorario di Federprivacy.*

La rivoluzione sul fronte dei pagamenti è alle porte. Dopo un 2014 dinamico e determinante per lo sviluppo della tecnologia e della normativa in materia di servizi di pagamento elettronici, che ha visto schierarsi uno dopo l'altro i maggiori players del settore, finalmente tutto è pronto per partire operativamente. A confermare la tendenza di questa crescita inarrestabile, è la recente ricerca condotta dall'Osservatorio *Mobile Payment & Commerce della School of Management* del Politecnico di Milano, presentata il 19 febbraio scorso, dal sintomatico titolo "*Mobile Payment*: la rivoluzione dei pagamenti è nel cellulare?". Sebbene i tempi non siano ancora maturi per parlare di un sistema diffuso, le potenzialità e le prospettive di sviluppo sono estremamente promettenti, complici la flessibilità di utilizzo e la praticità delle operazioni. Quel che è certo è che il *mobile payment* ha dato un ulteriore impulso al processo di digitalizzazione, determinando da un lato un'accelerazione nella dematerializzazione dei trasferimenti di denaro e dall'altro un ampliamento della tipologia di servizi e prodotti e degli attori coinvolti nei vari procedimenti.

Un passo decisivo a favore del pagamento con moneta elettronica è stato compiuto con l'evoluzione della normativa connessa al *Payment Service Directive* e con altre direttive sulla materia, determinanti per creare un comune terreno di azione a livello europeo ed un mercato omogeneo. Le origini si possono rintracciare nell'emanazione del D. Lgs del 2010, in recepimento della Direttiva Europea 2007/64/CE (*Payment Services Directive – PSD*), in occasione del quale venne esteso il mercato dei servizi di pagamento anche a operatori del settore non bancario, consentendo loro di agire come intermediari di pagamento, sebbene con minori adempimenti a cui sottostare rispetto agli istituti bancari.
Fornitori di reti e servizi di comunicazione elettronica accessibili al pubblico non sono stati compresi in questa categoria dal momento che hanno facoltà di operare senza rientrare negli adempimenti della PSD, a patto che non si limitino a praticare quale intermediario autorizzato del pagamento tra utente ed esercente, ma svolgano invece altre funzioni.

Il Provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di mobile remote payment, pubblicato in Gazzetta Ufficiale lo scorso 16 Giugno 2014, sarà certamente ricordato come una pietra miliare per lo sviluppo e l'evoluzione dei servizi in questo ambito. È proprio su tale importante documento che si concentrerà l'attenzione della breve disamina di seguito, ripercorrendo i punti focali della disposizione e soffermandoci sui soggetti coinvolti nel processo di gestione delle transazioni.

Occorre fare una breve introduzione propedeutica per comprendere il fertile contesto grazie al quale il mobile payment ha potuto svilupparsi e dar vita a nuove prospettive anche nel nostro Paese: entrando sin da subito nel vivo dell'argomento, il testo si concentra sulle operazioni eseguibili dagli utenti - identificate in due categorie principali - vale a dire il:

- ***Mobile remote payment***, effettuabile a distanza tra esercente e cliente per mezzo del telefono cellulare;
- ***Mobile proximity payment***, ovvero il pagamento eseguito dal cliente avvicinando il dispositivo mobile (dotato di tecnologia NFC, *Near Field Communication*) ad un apposito lettore messo a disposizione dall'esercente.

In entrambi i casi, l'utente dispone dei dati della propria carta di credito all'interno dello smartphone. Un portafoglio digitale a tutti gli effetti.

Per quanto riguarda i soggetti coinvolti nel processo vengono individuate tre maggiori categorie, rappresentanti: operatore, aggregatore e

merchant, ognuna delle quali risponde a specifici adempimenti.

La figura dell'operatore delinea il soggetto che fornisce alla "*propria clientela un servizio di pagamento tramite telefono cellulare per l'acquisto di contenuti digitali attraverso l'utilizzo di una carta telefonica ricaricabile*". L'aggregatore, invece, secondo quanto descritto dal Provvedimento, è costituto dal "*soggetto o i soggetti che mettono a disposizione e gestiscono la piattaforma abilitante per la fruizione della piattaforma di prodotti e servizi digitali*". Infine, con il termine merchant, si fa riferimento al fornitore dei contenuti digitali offerti all'utente.

Come risulta facilmente intuibile il sistema di pagamento elettronico presuppone il traffico e il trattamento di grandi quantità di informazioni riferibili all'utente, quali numero telefonico, dati anagrafici o informazioni connesse alla tipologia di servizio o prodotto acquistato. A questo si aggiungono ulteriori dati come quelli riferiti alle informazioni relative alla sottoscrizione e alla revoca del servizio e quelli, non meno importanti, di natura sensibile, riferiti alla fruizione del contenuto o del servizio.

Torniamo ai contenuti del Provvedimento emanato dall'Autorità Garante. Andando ad analizzare gli adempimenti a cui deve sottostare l'operatore, emerge primariamente l'obbligo della messa a disposizione agli utenti di un'informativa chiara e completa, obbligo che se non rispettato può comportare alte sanzioni amministrative. Il provvedimento pone l'accento sulla necessità di indicare con chiarezza le finalità di erogazione del servizio, specificando il da farsi "*se i dati personali dell'utente sono trattati anche per scopi ulteriori, ovvero per finalità di marketing, quali invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, specificando, se le suddette attività vengono effettuate anche attraverso il ricorso a modalità automatizzate di contatto (quali, ad esempio, fax, mail, sms o mms)*".

E qui si aprono scenari interessanti e "pericolosi" sotto il profilo della aderenza agli obblighi nomativi in merito alle finalità ed ai limiti di trattamento. Fondamentale il richiamo a eventuali trattamenti di profilazione o di comunicazione delle informazioni a terzi, compresa la trasmissione del numero telefonico al merchant che deve essere effettuata solo ai fini di una gestione ottimizzata del servizio o per le necessarie attività di assistenza. Attività di marketing, di profilazione e di comunicazione a terzi possono essere effettuate solo previa acquisizione del "*consenso espresso, libero e specifico dell'utente per ciascuna finalità del trattamento*", raccolto tramite un *flag* della specifica casella dell'informativa.

Nell'informativa si dovrà indicare il titolare del trattamento nonché la sussistenza del soggetto o dei soggetti designati responsabili, con specifico riferimento al ruolo dell'*hub* tecnologico, oltre all'eventuale utilizzo di dati di natura sensibile. L'informativa, quella breve, dovrà essere fornita all'utente e resa disponibile all'interno dell'apposita sezione della pagina *web* dell'operatore o nella *landing page*, mentre quella più dettagliata potrà essere consultata cliccando uno specifico *link*, sempre nella medesima pagina. Il Garante puntualizza che nel caso in cui la fruizione del contenuto o del servizio renda riconoscibile l'orientamento dell'utente comportando il trattamento di dati sensibili, è necessario un consenso scritto dell'interessato o manifestato con altra modalità telematica equiparabile.

Anche le misure di natura tecnica o organizzativa ricomprese nel Provvedimento dal Garante devono rispettare una serie di parametri a tutela della privacy degli utenti. Innanzitutto esse devono limitarsi a trasmettere all'operatore e/o al *merchant* le sole categorie merceologiche dei prodotti digitali acquistati, "*senza alcun riferimento allo specifico contenuto del prodotto o del servizio fornito*". Inoltre, nel caso di operazioni non andate a buon fine, i messaggi inoltrati al *merchant*, all'aggregatore (e in casi specifici all'operatore) devono indicare solo il buon fine o l'esito negativo della transazione, senza riferimenti specifici alle motivazioni del mancato completamento dell'azione, quale ad esempio l'insufficienza del credito sulla scheda – comunicata eventualmente all'utente stesso tramite un messaggio specifico. Tra le misure di sicurezza previste, si ricordano inoltre le forme di mascheramento nella trasmissione e visualizzazione dei dati per mezzo di meccanismi di cifratura e misure di *strong authentication* e di tracciamento per le attività eseguite dall'operatore di *customer care* e dall'aggregatore.

Con il sistema dei "meccanismi di rotazione", progettati per associare al medesimo utente chiavi di codifica differenti e in grado di celare i dati all'interno dei diversi processi di profilazione, è possibile impedire un eventuale controllo incrociato dell'utenza. Ulteriori misure di sicurezza riguardanti la fruizione di contenuti destinati ad un pubblico adulto prevedono "*l'attribuzione da parte dell'operatore al cliente, di cui abbia verificato la maggiore età, di un apposito codice numerico di accesso ovvero di un Pin dispositivo, unicamente ed esclusivamente associato di volta in volta alla particolare tipologia di prodotto o servizio di cui l'utente intende fruire*".

Spostando l'attenzione sul piano della conservazione dei dati, il Provvedimento prevede che i medesimi vengano conservati per un periodo di tempo limitato e comunque proporzionato rispetto alle finalità del trattamento, alla scadenza del quale l'operatore dovrà provvedere alla cancellazione dal sistema. In caso di ulteriore e specifica esigenza di conservazione a fronte di una contestazione anche in sede giudiziale, nel rispetto delle norme sulla materia, è possibile mantenere i dati per un periodo più lungo. Preme sottolineare come il concetto di "cancellazione" sia poco praticato e mal "digerito" in linea generale dai titolari del trattamento, in particolare laddove il dato sia stato raccolto con finalità ulteriori rispetto a quelle primarie. Eppure è bene tenere presente come si configuri la violazione di dati personali, anche nel caso di conservazione di dati che dovevano essere cancellati, vigendo il rispetto di quanto sancito dall'art. 32 bis del Codice e dal Provvedimento in materia di *data breach*.

A seguito della disamina sugli obblighi di informativa, raccolta del consenso, misure di sicurezza e conservazione dei dati in seno all'operatore del processo di *mobile payment*, il Garante indirizza la lente d'ingrandimento sull'attività degli aggregatori le cui competenze si concentrano sulla gestione del processo di acquisto del bene digitale, sull'operazione di disattivazione del servizio, sull'eventuale creazione di CRM per i *call center* di ciascun operatore, su una eventuale attività di reportistica destinata all'ambito *marketing* e sulla gestione del cosiddetto cruscotto *self*

care fruibile dall'utente per monitorare il dettaglio degli acquisti effettuati e degli addebiti connessi.

L'aggregatore è inoltre tenuto alla conservazione dell'intero elenco dei messaggi di attivazione e disattivazione. Per quanto riguarda l'informativa e il relativo consenso, egli ha meno vincoli rispetto all'operatore, non dovendosi interfacciare direttamente con l'utente finale. Ciò nondimeno ricade spesso nel suo campo d'azione la predisposizione per conto dell'operatore della landing page "prevista per il rilascio dell'informativa e dei consensi da richiedere all'utente" e l'acquisizione del consenso dell'utente per i dati forniti e utilizzati per finalità di *marketing* e/o profilazione, nel caso rivesta il ruolo di titolare del trattamento.

Il processo di gestione dell'operazione di acquisizione del servizio o del contenuto digitale a partire dalla corretta associazione tra il numero telefonico e l'operatore, passando per il reindirizzamento dell'utente su una pagina *web* del soggetto aggregatore, fino alla ricezione di un pin sul numero dell'utente in grado di abilitarlo all'acquisto una volta inserito nell'apposito form della pagina web, è parte integrante dei compiti soggetti alla gestione e alla responsabilità dell'aggregatore. Come rileva il Garante nel caso la piattaforma sia gestita da più aggregatori è essenziale rispettare specifiche misure di sicurezza sia per ragioni di confidenzialità del dato sia per l'esigenza di accuratezza del dato secondo cui, in caso di necessità, sia possibile la ricostruzione dello storico degli acquisiti entro 24 ore.
Per quanto riguarda le misure di sicurezza individuate e le norme in materia di conservazione vigono le medesime prescrizioni individuate con riguardo all'operatore.

L'ultima parte del Provvedimento si concentra, infine, sugli adempimenti del *merchant*, identificati attualmente come i soggetti che "*vendono prodotti editoriali, contenuti multimediali in modalità streaming, broadcasting e download, giochi, community e servizi inerenti, nonché servizi relativi a materiale a carattere sessuali*".
Tali servizi/contenuti possono essere fruiti dal cliente dal *web* o dal dispositivo mobile e, in certi casi, è prevista la registrazione dell'utente al sito *web* del *merchant*. **Numero di telefonia mobile, data e ora dell'operazione, descrizione del bene acquistato ed importo, identificativo della sessione e indirizzo ip ed eventuale indirizzo di posta elettronica dell'utente rappresentano le informazioni con cui viene a contatto il *merchant***, il quale è tenuto a fornire all'utente un'informativa dove siano evidenziate finalità della fornitura o del servizio e finalità ulteriori per le quali possono essere trattati i dati.

L'informativa deve inoltre rendere note "*eventuali attività di profilazione e marketing diretto, programmi di fidelizzazione, nonché trattamenti di comunicazione a terzi e fruizione dei contenuti digitali da cui possa dedursi un orientamento dell'utente che implichi un trattamento di dati di natura sensibile*", acquisendo per tali ipotesi, un consenso esplicito dell'utente e adottando - in ogni caso - adeguate misure di sicurezza a tutela delle informazioni trattate.

Tra queste, a titolo esemplificativo, ricordiamo quelle atte a garantire l'impossibilità di risalire alle informazioni relative alla mancanza o all'insufficienza del credito telefonico dell'utente oppure la disponibilità di decifrazione dei dati solo rispetto all'attività di assistenza.
Sul fronte della conservazione dei dati vigono le stesse considerazioni e relative prescrizioni individuate rispetto all'operatore.

In conclusione, possiamo dire che sul piano normativo tutto è pronto, almeno in questa fase iniziale, per gestire il passaggio al *mobile wallet*. La dinamicità del mercato gravitante intorno all'orbita del *digital payment* e la crescita degli operatori e delle offerte lasciano presagire grandi potenzialità di sviluppo per il futuro. Tuttavia se da un lato questa vivacità testimonia il grande interesse intorno la materia, dall'altro genera numerose incertezze soprattutto in termini di sicurezza delle operazioni e misure per scongiurare la perdita dei dati o il loro furto, alla stregua di qualsiasi altra transazione digitale o pagamenti elettronici tramite carta di credito.

Se da una parte l'attesa, rispetto agli operatori lato *business* su questo tema, è che vi sia attenzione al trattamento dei dati ed organizzazione dei processi che li caratterizzano, dall'altra vi è quasi la certezza che, lato *consumer*, sarà prestata poca attenzione, che al contrario ogni utente dovrebbe manifestare rispetto all'utilizzo del proprio *tablet* o *smartphone*, divenuto a tutti gli effetti il principale veicolo delle nostre relazioni professionali e private e delle informazioni personali, in molti casi anche riservate. Occorre dunque essere entusiasti di come le tecnologie possano semplificare ancor di più atti ordinari e quotidiani, ma allo stesso tempo sarebbe utile aumentare l'informazione e quindi creare una cultura effettiva circa il valore dell'identità digitale, valorizzando maggiormente la protezione dei dati e partendo da una reale consapevolezza di chi li rilascia. ©