**VEDI ANCHE**

- Comunicato stampa del 31 marzo 2015

- Comunicato stampa del 17 giugno 2014

**- Proroga del termine per l'attuazione delle prescrizioni del provvedimento n. 258 del 22 maggio 2014 in materia di mobile remote payment - 20 novembre 2014**

[doc. web n. 3161560]

**Provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di mobile remote payment - 22 maggio 2014**
*(Pubblicato sulla Gazzetta Ufficiale n. 137 del 16 giugno 2014)*

Registro dei provvedimenti
n. 258 del 22 maggio 2014

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

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

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

VISTA la direttiva 2007/64/CE del Parlamento europeo e del Consiglio del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno ("Payment Service Directive"), recante modifica delle direttive 97/7/CE; 2002/65/CE; 2005/60/CE e 2006/48/CE che abroga la direttiva 97/5/CE (di seguito PSD);

VISTO il decreto legislativo n. 11 del 27 gennaio 2010 (pubblicato sul Supplemento ordinario alla Gazzetta Ufficiale n. 36 del 13 febbraio 2010), di recepimento della PSD;

VISTA la direttiva 2009/110/CE, del Parlamento europeo e del Consiglio concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, ("e-Money Directive") recante modifica delle direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE (di seguito EMD);

VISTO il decreto legislativo n. 45 del 16 aprile 2012 (pubblicato sulla Gazzetta Ufficiale n. 99 del 24 aprile 2012), di recepimento della EMD;

VISTI i provvedimenti della Banca d'Italia del 5 luglio 2011 di "Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti e obblighi delle parti)" e del 15 febbraio 2010 recante le "Disposizioni di vigilanza per gli istituti di pagamento";

VISTO il Libro verde della Commissione europea dell'11 gennaio 2012 "Verso un mercato europeo integrato dei pagamenti tramite carte, internet e telefono mobile";

VISTA la Proposta di risoluzione del 20 novembre 2012 del Parlamento europeo sul Libro verde della Commissione europea;

VISTO il decreto legge n. 201 del 6 dicembre 2011, recante "Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici" (pubblicato sulla Gazzetta Ufficiale n. 284 del 6 dicembre 2011 – Suppl. Ordinario n. 251) c.d. "Decreto SalvaItalia", convertito con modificazioni dalla l. 22 dicembre 2011, n. 214 (pubblicata sulla Gazzetta Ufficiale n. 300 del 27 dicembre 2011 - Suppl. Ordinario n. 276) e, in particolare, l'art 12 (comma 4) "Riduzione del limite per la tracciabilità dei pagamenti a 1.000 euro e contrasto all'uso del contante" con riguardo ai nuovi prestatori di servizi di pagamento;

VISTO il decreto legge n. 179 del 18 ottobre 2012, recante "Ulteriori misure urgenti per la crescita del Paese" (pubblicato sulla Gazzetta Ufficiale n. 245 del 19 ottobre 2012 – Suppl. Ordinario n. 194/L), c.d. "Decreto sviluppo-bis", convertito con modificazioni dalla l. n. 221 del 17 dicembre 2012 (pubblicata sulla Gazzetta Ufficiale n. 294 del 18 dicembre 2012 – Suppl. Ordinario n. 208) e, in particolare, l'art. 8 "Misure per l'innovazione dei sistemi di trasporto" e l'art. 15 "Pagamenti elettronici" che, tra l'altro, ha sostituito, al comma 1, l'art. 5 del decreto legislativo 7 marzo 2005, n. 82 recante il "Codice dell'amministrazione digitale";

VISTO il decreto ministeriale n. 145 del 2 marzo 2006, "Regolamento recante la disciplina dei sevizi a sovrapprezzo" (pubblicato sulla Gazzetta Ufficiale n. 84 del 10 aprile 2006);

VISTO il Libro bianco dell'European Payments Council del 19 giugno 2013 sui sistemi mobili di pagamento (mobile wallet payments);

VISTA la "Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 2002/65/CE, 2013/36/UE e 2009/110/CE e che abroga la direttiva 2007/64/CE" della Commissione europea del 24 luglio 2013;

VISTI gli emendamenti del Parlamento Europeo alla suddetta proposta di direttiva, approvati il 3 aprile 2014;

VISTO il parere del Garante europeo della protezione dei dati sulla medesima proposta, pubblicato sulla Gazzetta ufficiale dell'Unione europea dell'8 febbraio 2014 (2014/C38/07) e sul sito del GEPD http://www.edps.europa.eu;

VISTA la 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)";

VISTA la direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 "riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE";

VISTA la decisione della Corte di Giustizia dell'Unione Europea dell'8 aprile 2014 n. 54/2014, in riferimento alle cause riunite C-293/12 e C-594/12, che ha dichiarato l'invalidità della direttiva 2006/24/CE;

VISTO il provvedimento del Garante del 15 maggio 2013 sul "Consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto" (pubblicato sulla Gazzetta Ufficiale n. 174 del 26 luglio 2013);

VISTO il provvedimento del Garante in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) del 4 aprile 2013 (pubblicato sulla Gazzetta Ufficiale n. 97 del 4 aprile 2013);

VISTO il d.P.R. del 28 dicembre 2000, n. 445, recante il Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (pubblicato sulla Gazzetta Ufficiale n. 42 del 20 febbraio 2001);

RITENUTO OPPORTUNO fornire le necessarie indicazioni rispetto al trattamento dei dati personali degli utenti che si avvalgono di servizi di pagamento o trasferimento di denaro tramite telefono cellulare, c.d. mobile payment;

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

RELATORE il dott. Antonello Soro;

**PREMESSO**

Il ricorso alle potenzialità del mobile payment, ovvero dei servizi che consentono di gestire gli acquisti ed i relativi pagamenti di beni sia digitali che fisici tramite un terminale mobile, la cui diffusione ha negli ultimi anni, grazie alla continua evoluzione della tecnologia, radicalmente modificato il settore del commercio tradizionale ed elettronico ha aperto, anche nel nostro Paese, nuove prospettive. Ciò ha determinato un'accelerazione della conclusione delle transazioni commerciali ed un'accentuazione dei processi di smaterializzazione dei trasferimenti di denaro, ampliando, altresì, la tipologia dei prodotti e servizi fruibili attraverso il ricorso al mobile payment e la platea dei soggetti che operano in questo ambito, nonché la quantità di dati personali trattati.

I servizi di mobile payment, classificabili nelle due principali categorie del mobile remote payment e del mobile proximity payment, riguardano, rispettivamente, le operazioni di pagamento di un bene o servizio tra esercente e cliente, attivate da quest'ultimo a distanza attraverso il telefono cellulare e le operazioni di pagamento eseguite dal cliente avvicinando il dispositivo mobile, dotato di tecnologia NFC (Near Field Communication che fornisce connettività wireless bidirezionale a corto raggio) ad un apposito lettore POS (point of sale), posto presso il punto vendita dell'esercente da cui si acquista il bene.

Si tratta di passi importanti nel settore dei micropagamenti rispetto all'uso del contante, da cui discendono valutazioni che riguardano anche il trattamento dei dati personali degli interessati.

Se infatti, da un lato, si pongono le facilitazioni delle modalità di acquisto attraverso il terminale mobile ed un possibile risparmio dei costi propri delle transazioni effettuate con carte di pagamento, dall'altro non possono trascurarsi i profili che investono il corretto utilizzo e la sicurezza delle informazioni di carattere personale che l'utente deve fornire per fruire dei nuovi servizi di pagamento.

Il mobile payment ed il conseguente ricorso sia a reti di comunicazione elettronica, sia a tecnologie come la NFC (che, con riguardo alla modalità proximity, saranno richiamate in un apposito provvedimento dell'Autorità) implica, infatti, il trattamento di una serie di dati personali dell'utente non solo di carattere identificativo ma, potenzialmente, anche di natura sensibile. Ciò con la conseguenza che tale trattamento, oltre a svolgersi nel rispetto della disciplina sulla protezione dei dati personali e, in particolare, dei principi generali di liceità, pertinenza e non eccedenza, di correttezza e buona fede sanciti dal Codice (cfr. art. 11 ), deve essere improntato anche al rispetto del presente provvedimento generale.

Il provvedimento dell'Autorità è difatti volto ad individuare le prescrizioni dirette ai diversi soggetti coinvolti nelle operazioni di pagamento tramite telefonia mobile, allo scopo di prevenire i rischi connessi ad un utilizzo improprio dei dati personali degli utenti che intendono avvalersi del mobile remote payment.

**1. Quadro normativo.**

La direttiva 2007/64/CE, c.d. PSD (recepita a livello interno dal d.lg. n. 11/2010), ha aperto il mercato dei servizi di pagamento anche ad operatori di matrice non bancaria nell'ottica, non solo di armonizzare il relativo quadro giuridico, superando la frammentazione normativa delle singole realtà nazionali, ma di definire nuovi profili di efficienza, parità e sicurezza per tutti i portatori di interessi in tale ambito.

La PSD indica, tra l'altro, le condizioni per autorizzare i nuovi soggetti non bancari all'esercizio di un servizio di pagamento all'interno dell'UE, prevedendo, in particolare, che i nuovi istituti di pagamento possano operare come intermediari di pagamento, previa autorizzazione delle Autorità competenti, nell'ambito di un "regime semplificato" rispetto a quello degli istituti bancari.

Difatti, nella sua attuale configurazione, la direttiva, nel definire i "servizi di pagamento" rimandando alle attività commerciali elencate nel relativo allegato (cfr. art. 4, punto 3 che rinvia al punto 7 dell'Allegato) consente agli operatori del sistema o della rete di telecomunicazioni o digitale o informatica di agire nella veste di intermediari tra l'utilizzatore di servizi di pagamento che usa un dispositivo di telecomunicazione digitale o informatico ed il fornitore di beni e servizi (cfr. anche l'art. 1, comma 1, lett. b), punto 7 del decreto interno di recepimento). Tale attività rientra nell'ambito di quelle definite nel c.d. positive scope.

Dal perimetro di applicazione delle previsioni comunitarie e delle conseguenti disposizioni interne restano invece escluse le operazioni di pagamento, eseguite tramite il suddetto dispositivo, che si riferiscono all'acquisto di beni e servizi digitali, la cui consegna o il cui utilizzo siano effettuati mediante tale dispositivo gestito dall'operatore di telecomunicazione digitale o informatico, quando quest'ultimo non agisca esclusivamente come mero intermediario autorizzato del pagamento tra l'utente ed il fornitore di beni e servizi (cfr. l'art. 3, lett. l) della PSD e l'art. 2, comma 2, lett. n) del d.lg. n. 11/2010, a sua volta richiamato al par. 2.2.9 del menzionato provvedimento della Banca d'Italia del 5 luglio 2011), ma svolga una serie di ulteriori funzioni.

Tali funzioni possono rinvenirsi in quelle di accesso, ricerca e distribuzione del contenuto digitale e si atteggiano in modo tale che la relativa assenza non consentirebbe all'utente di fruirne con le medesime modalità sopra descritte. Viene così a delinearsi il c.d. negative scope, ovvero lo spazio delle deroghe nel quale ricadono quelle attività non classificate come servizi di pagamento che possono essere prestate dagli operatori del sistema o della rete di telecomunicazioni o digitale o informatica (da intendersi come fornitori di reti e servizi di comunicazione elettronica accessibili al pubblico), senza l'obbligo di diventare o agire come un intermediario di pagamento.

Tale esclusione consente quindi all'operatore, sotto un profilo di significativa innovazione, di intervenire nel settore dei pagamenti elettronici anche prestando direttamente un servizio attraverso la propria rete di telecomunicazione.

In questo senso la PSD (Considerando 6), nel precisare l'opportunità che il quadro giuridico disciplinato non si applica quando l'attività dell'operatore va al di là della semplice operazione di pagamento, richiama le menzionate funzioni di accesso, distribuzione o consultazione proprio in termini di "valore intrinseco" che tale soggetto può aggiungere al contenuto dei beni digitali offerti all'utente.

**2. Futuri inquadramenti normativi.**

Con riguardo al quadro normativo sopra delineato occorre dar conto dei recenti cambiamenti previsti a livello europeo, rispetto al vigente acquis legislativo e regolamentare in materia di servizi di pagamento.

Ci si riferisce alla proposta della Commissione europea del 24 luglio 2013 di riesame della "e-Money Directive" e di inglobamento ed abrogazione della "Service Payment Directive", al precipuo scopo di aggiornare l'assetto giuridico in materia di servizi di pagamento nell'ambito dell'UE, "in un'epoca in cui la distinzione tra istituti di pagamento e istituti di moneta elettronica è sempre meno netta e si assiste alla convergenza delle tecnologie e dei modelli commerciali" e di rispondere al meglio alle esigenze di un vero e proprio mercato integrato che favorisca la concorrenza, l'innovazione e la sicurezza.

Tali obiettivi erano del resto già emersi nel gennaio 2012, a seguito della pubblicazione, da parte della Commissione, del Libro Verde "Verso un mercato europeo integrato dei pagamenti tramite carte, internet e telefono mobile", nonché degli esiti della successiva consultazione pubblica che aveva registrato un ampio numero di contributi sulle possibili esigenze di modifica del vigente quadro dei pagamenti.

Alla luce degli scopi e degli ostacoli individuati nel Libro verde, il Parlamento europeo ha poi, con la risoluzione adottata il 20 novembre 2012, richiesto una riforma del modello di governance dell'area unica dei pagamenti in euro, in linea con l'agenda digitale e, in particolare, con la creazione di un mercato unico del digitale.

In questo quadro, l'analisi condotta nell'ambito della menzionata proposta di inglobamento ed abrogazione della PSD ha fatto emergere, tra l'altro, l'intenzione di ridefinire il dettato degli artt. 3 e 4 della direttiva tanto sotto il profilo soggettivo, quanto sotto quello oggettivo, evidenziando una nuova, possibile, prospettiva che tende a delimitare l'esenzione relativa ai contenuti digitali esclusivamente ai servizi di pagamento accessori, prestati dai fornitori di reti o di servizi di comunicazione elettronica sulla base di determinate soglie di pagamento.

Ciò nondimeno, in attesa di conoscere se e quali saranno gli effettivi esiti della proposta e che implicazioni essa comporterà nel nostro ordinamento interno, giova ribadire che lo scopo del presente provvedimento, il quale si basa sull'attuale assetto normativo del settore, 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.

In quest'ottica l'Autorità ha peraltro condotto una serie di attività ispettive nell'ambito della fornitura di servizi di mobile remote payment, così da individuare eventuali profili di criticità e prevedere misure opportune e sempre più mirate ad una tutela effettiva dei dati personali, fornendo altresì utili strumenti di intervento a tutti i soggetti coinvolti.

**3. Il Mobile remote payment.**

Attualmente le operazioni di mobile remote payment, ricorrendo le circostanze sopra menzionate, vedono coinvolti diversi soggetti, tra cui i fornitori di reti e servizi di comunicazione elettronica accessibili al pubblico, per l'acquisto di contenuti digitali tramite terminale mobile, ovvero, anche a seguito degli interventi normativi di cui al citato "Decreto Sviluppo bis", di titoli digitalizzati che possono consentire all'utente l'accesso a servizi di utilità sociale o a servizi in mobilità. Rispetto a questi ultimi i profili legati al trattamento dei dati personali saranno oggetto di un apposito provvedimento del Garante, così come altre considerazioni dell'Autorità potranno investire ambiti di utilizzo di dati personali che prevedono il ricorso a tecnologie diverse e tradizionali e altri servizi di pagamento.

Pertanto, proprio in uno scenario così in evoluzione, si è ritenuto opportuno individuare, nell'ambito del presente provvedimento, un contesto operativo, un'architettura tecnico-organizzativa di riferimento ed i possibili ruoli dei soggetti coinvolti nel processo di erogazione del servizio di mobile remote payment.

In particolare, l'ambito individuato riguarda l'offerta da parte dei fornitori di reti e servizi di comunicazione elettronica accessibili al pubblico (di seguito operatori) di prodotti e di servizi digitali (singoli prodotti o servizi in abbonamento) fruibili dall'utente tramite smartphone, tablet e PC, attraverso servizi di micropagamento (secondo quanto previsto dal d.m. n. 145/2006) mediante terminale mobile.

La menzionata architettura prevede la costituzione di una apposita piattaforma tecnologica destinata alla gestione delle nuove modalità di pagamento attraverso l'addebito e la conseguente decurtazione del costo del contenuto digitale richiesto dal credito telefonico, per gli utenti dotati di una carta ricaricabile, ovvero l'addebito sul conto telefonico, per quelli che abbiano sottoscritto un contratto di abbonamento con l'operatore di riferimento.

I processi gestionali legati all'operatività della piattaforma implicano, infine, sotto il profilo soggettivo, l'intervento, oltre che degli operatori e dei fornitori dei contenuti digitali disponibili (di seguito merchant), di appositi hub preposti a svolgere generalmente, tra gli uni e gli altri, il ruolo di "interfaccia" tecnologica (di seguito aggregatori).

Le suddette considerazioni non intendono, tuttavia, limitare l'applicazione del presente provvedimento, il quale si rivolge all'intero contesto in cui può realizzarsi un'operazione di mobile remote payment volta all'acquisto di beni e servizi digitali, quindi anche attraverso altri scenari tecnologici ed altre configurazioni soggettive. Difatti sono da considerarsi ricompresi, nell'ambito di riferimento delle misure che vengono indicate dall'Autorità, anche altri soggetti diversi dagli operatori telefonici, dai merchant e dagli aggregatori, i quali, tramite proprie applicazioni ovvero applicazioni sviluppate da terze parti abilitate, consentono l'accesso ad un mercato di beni digitali, offrendo all'utente la possibilità di acquistare contenuti, giochi o programmi informatici di varia natura mediante l'utilizzo del credito telefonico.

**4. Ambito soggettivo.**

Come evidenziato, nel contesto dei servizi di mobile remote payment attualmente offerti agli utenti può individuarsi la figura dell'operatore che, alla luce della disciplina comunitaria ed interna, è in grado di fornire alla propria clientela un servizio di pagamento tramite telefono cellullare per l'acquisto di contenuti digitali attraverso l'utilizzo di una carta telefonica ricaricabile, ovvero sulla base di un abbonamento telefonico.

Accanto a tale soggetto, lo scenario si può arricchire, come detto, della presenza di altri player come l'aggregatore, ovvero il soggetto o i soggetti che mettono a disposizione e gestiscono la piattaforma abilitante per la fruizione dei prodotti e servizi digitali ed il merchant, ovvero il fornitore dei contenuti digitali offerti a vario titolo all'utente.

Utente o cliente è invece il soggetto titolare di una USIM prepagata o postpagata.

**5. Tipologia dei dati trattati.**

Rispetto alla tipologia dei dati trattati nell'ambito del mobile remote payment si è detto che il pagamento dei contenuti digitali avviene attraverso il telefono mobile e che il cliente può fruirne sia direttamente sul proprio smartphone, sia su altri tipi di terminali (ad es. tablet e PC).

Attraverso il mobile remote payment vengono trattate numerose informazioni riferibili all'utente che riguardano, in particolare, i dati relativi alla numerazione telefonica, i dati anagrafici, i dati legati alla tipologia del servizio o del prodotto digitale richiesto ed al relativo importo.

Ad essi si aggiungono i dati inerenti alla sottoscrizione ed alla revoca del servizio, quelli relativi agli addebiti degli acquisti nella fattura o sulla carta prepagata e, eventualmente, quelli di posta elettronica richiesti per una maggiore fruibilità del contenuto digitale, nonché l'indirizzo IP dell'utente.

Ai suddetti dati se ne possono peraltro aggiungere altri, anche di natura sensibile (cfr art. 4 comma 1, lett. d) del Codice), legati alla fruizione del contenuto o del servizio digitale.

Stante la varietà e molteplicità dei dati suscettibili di trattamento nel quadro delle operazioni sopra descritte possono, quindi, facilmente emergere profili di rischio per i diritti e le libertà fondamentali, nonché per la dignità dei soggetti interessati.

**6. Gli adempimenti dell'"operatore".**

*6.1. Descrizione dell'attività.*

Come già rilevato nelle premesse del presente provvedimento l'offerta di contenuti digitali, fruibili dall'utente su smartphone, tablet, personal computer, notebook e laptop, tramite il proprio credito telefonico può essere resa disponibile da parte dell'operatore, attraverso un'apposita piattaforma tecnologica.

I beni e servizi digitali proposti possono essere diversi e, riguardare ad esempio, copie di quotidiani on-line (one shot o in abbonamento), contenuti musicali e video, social games, contenuti riferiti ad un "pubblico adulto".

La gestione della piattaforma abilitante può essere affidata ad uno o più soggetti tecnologici il cui ruolo consiste nella messa a punto di un'interfaccia tra i merchant e gli operatori che consente all'utente di acquistare il contenuto digitale e di portare a termine l'operazione di pagamento, previa decurtazione del costo dalla scheda prepagata, ovvero addebito in abbonamento.

*6.2. Informativa*

Con riguardo alle operazioni di acquisto di beni e servizi digitali attraverso il mobile remote payment l'operatore deve rendere agli utenti un'informativa chiara e completa degli elementi di cui all'art. 13 del Codice.

In particolare, oltre al richiamo alla finalità di erogazione del servizio attraverso la nuova modalità, l'informativa deve specificare 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 (ex artt. 7, comma 4, lett. b) e 140 del Codice), specificando, se le suddette attività vengono effettuate anche attraverso il ricorso a modalità automatizzate di contatto (quali, ad esempio, fax, email, sms o mms).

Un ulteriore richiamo deve riguardare i trattamenti di profilazione, anche nell'ambito di eventuali programmi di fidelizzazione e di comunicazione dei dati a soggetti terzi.

Rispetto a tale ultimo profilo l'informativa deve chiarire che la trasmissione del numero di telefonia mobile dell'utente al merchant nell'ambito delle operazioni di mobile remote payment è effettuata esclusivamente per consentire a quest'ultimo un'efficace gestione del servizio con riferimento alle necessarie attività di assistenza alla clientela.

Sia nel caso in cui vengano svolte attività di marketing, sia in quello in cui si effettui un'attività di profilazione o, ancora, di comunicazione dei dati a terzi, nell'informativa rilasciata dall'operatore dovrà risultare chiaramente che dette attività possono svolgersi solo previa acquisizione del consenso espresso, libero e specifico dell'utente per ciascuna finalità del trattamento, sulla base di quanto dispone l'art. 23 del Codice e, nel caso in cui si ricorra a modalità automatizzate di contatto, sulla base dell'art. 130 del Codice, tenuto conto di quanto evidenziato dall'Autorità nel citato provvedimento del 15 maggio 2013 (pubblicato anche sul sito istituzionale www.garanteprivacy.it, doc. web. n. 2543820).

Un'ulteriore, espressa, indicazione deve poi riguardare l'esercizio da parte dell'utente dei diritti sanciti dall'art. 7 del Codice.

Nell'informativa deve inoltre emergere la chiara indicazione del titolare del trattamento e del soggetto o dei soggetti designati responsabili ai sensi dell'art. 29 del Codice, in particolare avuto riguardo al ruolo dell'hub tecnologico che può anche agire in veste di responsabile esterno del trattamento, nonché dei soggetti incaricati del trattamento ai sensi dell'art. 30 del Codice. Analogamente, deve risultare chiaro all'utente l'eventuale rapporto di co-titolarità tra l'operatore ed il merchant.

L'informativa deve anche richiamare l'eventuale utilizzo di dati di natura sensibile da parte dell'operatore e le relative modalità di trattamento.

L'informativa deve essere rilasciata al momento dell'iscrizione o adesione dell'utente ai servizi fruibili tramite mobile remote payment.

Posti i vincoli di spazio, legati alle dimensioni degli schermi dei terminali mobili normalmente utilizzati per la fruizione di tali servizi, all'informativa deve essere data idonea evidenza adottando, in particolare, una formula basata sull'approccio c.d. layered, ovvero a strati.

In tal senso, all'utente dovrà essere fornita una prima informativa breve, contenente il riferimento agli elementi essenziali del trattamento (tra i quali almeno, l'indicazione delle finalità e gli estremi identificativi del titolare), da inserirsi all'interno di un'apposita sezione della pagina web dell'operatore, ovvero nella landing page predisposta dall'aggregatore ed un'ulteriore informativa, più lunga e dettagliata, alla quale il cliente potrà accedere selezionando, nella suddetta pagina, uno specifico link.

*6.3. Consenso.*

Il consenso al trattamento dei dati personali dell'utente che fruisce del servizio di mobile remote payment non è necessario ai fini della relativa fornitura, stante il disposto dell'art. 24, comma 1, lett. b) del Codice.

In veste di titolare del trattamento l'operatore deve invece acquisire il consenso dell'utente nel caso in cui i dati forniti da quest'ultimo, riferibili agli acquisti effettuati, vengano utilizzati per finalità di marketing diretto e/o per finalità di profilazione, anche nell'ambito di eventuali programmi di fidelizzazione. Il consenso dell'utente deve essere richiesto anche nel caso di comunicazione dei dati a soggetti terzi.

Rispetto alle suddette finalità l'utente deve rilasciare specifici e distinti consensi, secondo quanto disposto dal citato art. 23 del Codice e dall'art. 130 nel caso in cui si ricorra a modalità automatizzate di contatto.

Il consenso dell'utente può essere espresso tramite un flag da inserire in una specifica casella presente in una apposita sezione della pagina web dell'operatore, ovvero nella landing page predisposta dall'aggregatore, oppure attraverso altre idonee modalità informatiche.

Laddove dalla fruizione del contenuto o del servizio digitale sia possibile dedurre un orientamento dell'utente che implichi il trattamento di dati di natura sensibile, il consenso dell'interessato deve essere manifestato per iscritto, ovvero con altra modalità telematica equiparabile allo scritto, nel rispetto di quanto previsto dall'art. 26, comma 1, del Codice. In tal senso la modalità telematica equiparabile allo scritto può implicare, oltre al ricorso ad un documento sottoscritto con firma elettronica qualificata o digitale, anche il ricorso a forme alternative più diffuse, secondo quanto previsto dal menzionato d.P.R. n. 445/2000.

In ogni caso resta ferma la possibilità, per il titolare del trattamento, di individuare forme alternative di manifestazione del consenso che possano supplire alle modalità previste dalla normativa e che l'Autorità si riserva di valutare ai sensi dell'art. 17 del Codice.

*6.4. Dati trattati. Misure di sicurezza.*

A seguito dell'avvio dell'operazione di acquisto del bene digitale l'operatore, oltre al numero di telefonia mobile dell'utente, ai relativi dati anagrafici e a quelli legati al contratto di attivazione del servizio, acquisisce i dati relativi alla data e all'ora dell'operazione, nonché quelli che riguardano l'indicazione del prodotto digitale richiesto ed il relativo importo.

Le categorie merceologiche di riferimento dei prodotti digitali offerti sono normalmente definite dal merchant il quale deve limitarsi a trasmetterle all'operatore senza alcun riferimento allo specifico contenuto del prodotto o servizio fornito.

In tal senso, una misura che anche l'operatore deve adottare, al fine di garantire il corretto trattamento delle informazioni relative al prodotto o servizio richiesto dall'utente è quella di utilizzare tabelle interne di classificazione che prevedano criteri di codifica dei prodotti e servizi basati non sul loro specifico contenuto, ma esclusivamente sull'individuazione di classi e/o genere (ad es. video sportivo, cronaca etc.).

Tuttavia, nel caso di servizi in abbonamento, l'operatore può conoscere il nome del servizio acquistato dall'utente al fine di poter distinguere tra più abbonamenti dello stesso tipo e fornirgli informazioni, effettuare disattivazioni dal servizio stesso, nonché effettuare una corretta attività di fatturazione.

L'operatore gestisce il numero di telefonia mobile dell'utente anche per effettuare le necessarie verifiche sotto il profilo della sussistenza o meno di credito telefonico, a tal fine invia al merchant un messaggio di ok o ko a seconda che l'operazione sia andata o meno a buon fine.

Tale messaggio non deve tuttavia risultare accompagnato da codici che consentano di risalire puntualmente a cause ostative, diverse da quelle tecniche (ad esempio problemi di rete), legate all'indisponibilità od insufficienza di credito telefonico. Ciò al fine di evitare che sia il merchant che l'aggregatore vengano a conoscenza di informazioni riferite ad un dato economico dell'utente che non ha alcun rilievo sotto il profilo della gestione dell'operazione di mobile payment e che risulta ultroneo rispetto alle finalità del trattamento che i menzionati soggetti sono chiamati a svolgere.

Pertanto, il segnale di ko che l'operatore invia può essere accompagnato, da un codice che permetta solo di distinguere, tra le diverse causali di errore, quelle che danno luogo ad un retry da quelle che, invece, non prevedono la ripetizione della transazione.

Generalmente quando l'operazione effettuata non va a buon fine l'operatore può inviare all'utente un sms il quale, oltre a segnalare che si è verificato un errore durante l'operazione, con l'invito a controllare le proprie informazioni personali e ad effettuare un nuovo tentativo, evidenzia anche che il numero fornito non sembra essere abilitato a procedere all'acquisto.

Inoltre, se la causa del mancato acquisto è imputabile alla mancanza o insufficienza di credito telefonico, all'utente può pervenire un ulteriore messaggio che segnali l'insufficienza di credito sulla sim.

Con specifico riguardo ai dati presenti nella piattaforma dell'operatore utilizzata per le operazioni di mobile remote payment, quest'ultimo deve poi adottare, oltre alle misure di sicurezza dei dati e dei sistemi previste dall'art. 31 e segg. del Codice, nonchè dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'All. B) dello stesso, ulteriori cautele.

In particolare, è necessario che l'operatore preveda una forma di mascheramento dei dati, ad esempio mediante applicazione di un meccanismo crittografico (c.d. hash) le cui chiavi di decifrazione siano nella disponibilità dei propri addetti esclusivamente con riguardo alle operazioni di customer care.

Gli addetti all'attività di customer care, infatti, devono essere posti in grado di visualizzare, per finalità di assistenza alla clientela, lo storico di tutte le operazioni di acquisto effettuate da un determinato numero telefonico, i riferimenti temporali ed i relativi importi, nonché la categoria merceologica e la classe di prodotto o servizio digitale acquistato.

Ciò nondimeno, per l'accesso alle predette interrogazioni tali soggetti, che devono essere nominati incaricati del trattamento ai sensi dell'art. 30 del Codice, devono essere sottoposti ad una procedura di autenticazione basata su token e account nominale, con attribuzione dello specifico profilo "operatore di customer care" (c.d. strong authentication). Gli stessi devono essere altresì abilitati all'uso di un numero limitato di chiavi di interrogazione del sistema in merito alle operazioni da effettuare, costituito, recependo i contributi pervenuti a seguito della consultazione pubblica, esclusivamente dal numero di telefonia mobile del cliente, dal codice fiscale o dalla partita Iva, escludendo in tal modo forme di "ricerca inversa" che utilizzino come chiave i dati identificativi del bene digitale. Le operazioni di accesso al sistema

devono inoltre essere sottoposte a tracciamento analitico e dettagliato.

Tale ultima misura risulta oltremodo necessaria laddove l'operatore utilizzi un'unica piattaforma di provisioning sulla quale confluiscono tutti i dati relativi alle operazioni effettuate, non solo rispetto ai servizi di mobile remote payment, ma anche ad altri servizi erogati quali, ad esempio, quelli a valore aggiunto (c.d. VAS), con la conseguenza che il tracciamento deve estendersi a tutti i profili di autorizzazione impostati sulla predetta piattaforma.

Del resto, la previsione di una strong authentication e di file di log che consentano di risalire all'incaricato che effettua gli accessi al sistema si rivela idonea ad offrire un'adeguata protezione anche a quelle informazioni personali, dalle quali si possa dedurre un orientamento dell'utente che implichi un trattamento di dati di natura sensibile.

Dal momento che i fornitori di reti e servizi di comunicazione elettronica accessibili al pubblico, oltre a trattare i dati relativi alle operazioni di mobile remote payment ed alle scelte di consumo dei contenuti digitali, trattano anche dati di consumo/traffico telefonico e dati relativi alla fornitura di altre tipologie di beni digitali (quali ad esempio quelli legati alla c.d. Tv interattiva) per finalità di profilazione e marketing, risulta opportuno prevedere l'adozione di alcune misure ed accorgimenti anche nell'ottica di un'eventuale integrazione tra le diverse tipologie di dati e, quindi, di un'analisi incrociata delle abitudini, dei gusti e delle preferenze di consumo della clientela nei diversi ambiti individuati.

Infatti, tra i dati che normalmente identificano l'utente nei sistemi degli operatori sono presenti, oltre ai dati relativi alla linea di rete fissa, anche altri dati come il numero di telefonia mobile e l'indirizzo di posta elettronica, i quali potrebbero essere facilmente utilizzati come chiave comune tra i diversi sistemi dedicati alle differenti attività di profilazione dell'utenza, proprio al fine di far emergere fenomeni di correlazione tra consumi telefonici e consumi di beni digitali, fruiti anche con modalità mobile remote payment.

In tal senso, al fine di impedire un'eventuale profilazione incrociata dell'utenza, devono essere individuati appositi "meccanismi di rotazione" che consentano di applicare allo stesso utente chiavi di codifica differenti, destinate a mascherare i relativi dati all'interno dei diversi sistemi dedicati alle attività di profilazione che l'operatore può svolgere.

Con riguardo poi al trattamento dei dati che l'operatore può realizzare nell'ambito di eventuali programmi di fidelizzazione proposti all'utente, è necessario precisare che tali programmi devono basarsi esclusivamente su dati cumulati di spesa e non riguardare il singolo dato relativo allo specifico evento di acquisto del prodotto digitale effettuato dallo stesso.

*6.5. Particolari tipologie di contenuti. Misure di sicurezza.*

Tra i contenuti e i servizi digitali che l'utente può acquistare con la modalità mobile remote payment possono rientrare anche quelli, ad esempio destinati ad un pubblico adulto, per la cui fruizione risulta necessaria la previsione di apposite misure di sicurezza, come, ad esempio, 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, univocamente ed esclusivamente associato di volta in volta alla particolare tipologia di prodotto o servizio di cui l'utente intende fruire.

Un'ulteriore cautela di cui prevedere l'adozione è quella relativa all'implementazione di misure tecniche che garantiscano all'utente la possibilità di disattivare ogni servizio, destinato ad esempio ad un pubblico adulto, per default, nonché previo contatto con il servizio di customer care dell'operatore.

*6.6. Conservazione.*

I dati trattati nell'ambito delle operazioni di mobile remote payment devono essere conservati per un limitato periodo di tempo, proporzionato alle finalità realizzate con il trattamento, le quali non si esauriscono con la definizione del processo che conduce all'acquisto del contenuto digitale, ma si estendono alla gestione di attività correlate quali la fatturazione e quelle di carattere amministrativo e contabile. In considerazione di ciò, il periodo massimo di conservazione dei dati personali è individuato in sei mesi.

Alla scadenza del suddetto periodo l'operatore deve pertanto provvedere alla cancellazione dei dati dai propri sistemi, ferma restando l'ulteriore, specifica, conservazione necessaria in presenza di una contestazione anche in sede giudiziale e avuto riguardo alla disciplina sulla conservazione dei dati di traffico per fini di giustizia.

Ai fini della decorrenza del previsto periodo di conservazione si ritiene inoltre necessario differenziare gli acquisti di prodotti digitali c.d. one shot dagli abbonamenti, posto che per questi ultimi detto periodo deve cominciare a decorrere dalla scadenza dell'abbonamento stesso.

Analogamente, in presenza di una violazione di dati personali, l'operatore sarà tenuto al rispetto di quanto espressamente sancito dall'art. 32 bis del Codice, nonché dal citato provvedimento dell'Autorità del 4 aprile 2013 in materia di c.d. data breach (in www.garanteprivacy.it, doc. web n. 2388260).

**7. Adempimenti dell'"aggregatore".**

*7.1. Descrizione dell'attività.*

Come si è già evidenziato, l'aggregatore o hub tecnologico, è normalmente il soggetto (o i soggetti) cui è affidata la realizzazione di una serie di attività legate alla operatività della piattaforma tecnica che rende disponibili contenuti digitali attraverso il ricorso al mobile remote payment.

All'aggregatore può competere infatti, tra le possibili attività da svolgere, la gestione del processo di acquisto del bene digitale e del processo

di disattivazione del servizio, la creazione dell'interfaccia di customer relationship management destinata ai call center di ciascun operatore, l'eventuale attività di reportistica destinata alla funzione marketing, nonché la gestione di un cruscotto self care attraverso il quale il singolo utente può verificare, in ogni momento, il dettaglio dei propri acquisti e dei relativi addebiti. Tale ultima modalità può consentire inoltre, allo stesso utente di disattivare il servizio, nonché all'aggregatore di fornire un'apposita interconnessione che permette anche ai customer care degli operatori la consultazione dello storico degli acquisti effettuati dai clienti con i diversi merchant.

Nell'ambito dell'attività di gestione all'aggregatore è poi generalmente attribuita la funzione di conservazione di tutti gli sms di attivazione e disattivazione del servizio.

Con specifico riguardo all'attività di reportistica l'aggregatore può provvedere anche alla realizzazione dei report di verifica che contengono, in forma aggregata, i dati relativi al totale delle transazioni effettuate dagli operatori in un determinato lasso di tempo, nonché i dati inerenti alla spesa complessiva realizzata rispetto ad ogni singolo merchant. Detti report vengono normalmente inviati sia agli operatori che ai merchant. L'invio a questi ultimi permette infatti di valutare tutti i dati relativi agli acquisti, ai fini dell'emissione delle relative fatture e della definizione degli importi da percepire una volta detratte le royalties destinate agli operatori.

Su richiesta dell'operatore, l'aggregatore può produrre anche un report dettagliato sui clienti che hanno effettuato degli acquisti sui siti web dei merchant attraverso il mobile remote payment, con indicazione del numero di telefonia mobile e del prodotto o servizio digitale acquistato.

In tal caso, le informazioni che l'aggregatore invia all'operatore, con riguardo al prodotto o servizio digitale, non devono riguardare lo specifico contenuto richiesto dall'utente, ma riferirsi esclusivamente alla classe o al genere di appartenenza del servizio o prodotto, ovvero al servizio in abbonamento.

*7.2. Informativa.*

Tutte le attività connesse alla gestione della piattaforma tecnologica possono essere svolte dall'aggregatore in veste di responsabile esterno del trattamento dei dati personali, designato sia dall'operatore, sia dal merchant ai sensi dell'art. 29 del Codice. Conseguentemente, i suddetti soggetti sono tenuti ad indicare, nell'informativa da rilasciare agli utenti in qualità di titolari del trattamento, gli estremi identificativi dell'aggregatore che agisca come responsabile esterno del trattamento stesso (cfr. art. 13, comma 1, lett. f) del Codice).

In questa veste l'aggregatore può anche predisporre, per conto dell'operatore, la landing page prevista per il rilascio dell'informativa e dei consensi da richiedere all'utente.

In alcuni casi all'aggregatore può essere riconosciuta, sulla base di specifici accordi contrattuali con l'operatore ed il merchant, la possibilità di rendere direttamente disponibili i prodotti e i servizi normalmente offerti da quest'ultimo. A tal fine l'aggregatore può svolgere una serie di attività quali l'organizzazione e l'offerta del contenuto digitale al cliente, l'assistenza al medesimo (in genere previa attivazione di un apposito numero telefonico e/o di un indirizzo e-mail), la realizzazione di eventuali campagne o iniziative di comunicazione promozionale sul contenuto digitale offerto.

In tale veste l'aggregatore opera come titolare autonomo del trattamento e deve provvedere a rilasciare all'utente un'adeguata ed esaustiva informativa ai sensi dell'art. 13 del Codice anche ai fini dell'esercizio dei diritti di cui all'art. 7 del Codice da parte dell'interessato.

L'informativa, oltre a contenere tutti gli elementi già previsti con riguardo agli adempimenti individuati in capo all'operatore, deve anche essere adeguatamente evidenziata secondo le modalità già individuate.

*7.3. Consenso.*

Come già evidenziato, il consenso al trattamento dei dati personali dell'utente che fruisce del servizio di mobile remote payment non è necessario ai fini della relativa fornitura, analogamente non deve essere richiesto dall'aggregatore per altre finalità realizzate in veste di responsabile esterno del trattamento.

Laddove, invece, l'aggregatore rivesta il ruolo di titolare del trattamento la necessità di acquisire il consenso dell'utente sussiste nel caso in cui i dati forniti da quest'ultimo vengano utilizzati per finalità di marketing diretto e/o per finalità di profilazione, anche nell'ambito di eventuali programmi di fidelizzazione, o per comunicazioni a terzi, cosi come nell'ipotesi in cui dalla fruizione del contenuto si possa dedurre un orientamento dell'utente che implichi un trattamento di dati di natura sensibile. In questi casi operano, con riguardo al consenso ed alle relative modalità di rilascio, tutte le disposizioni già individuate rispetto al trattamento svolto dall'operatore, nonché tutte le considerazioni espresse dall'Autorità.

*7.4. Modalità di erogazione del servizio. Misure di sicurezza.*

L'operazione di acquisto tramite mobile remote payment può comportare l'utilizzo da parte dell'aggregatore di diverse modalità di riconoscimento del numero telefonico associato al cliente.

Una modalità automatica che si attiva nel caso in cui l'utente, una volta avuto accesso al sito del merchant (e, quindi, del medesimo hub che offre l'interfaccia tecnologica) per l'individuazione e la selezione del contenuto digitale di cui intende fruire, utilizzi per l'acquisto (mediante smartphone, tablet o dispositivo senza fili) la rete mobile di un operatore collegato alla piattaforma abilitante.

In tal caso, l'associazione tra il terminale mobile ed il numero di telefonia mobile avviene immediatamente e l'aggregatore acquisisce il numero dell'utente direttamente dall'operatore, il quale provvede anche alla verifica della disponibilità di credito. Al termine dell'operazione

il cliente riceve un sms che conferma l'avvenuto acquisto del prodotto o l'attivazione del servizio in abbonamento.

Un'ulteriore modalità che si attiva, invece, qualora l'utente acceda al sito del merchant, nonché dell'hub, da una rete diversa da quella dell'operatore (come una linea wi-fi, ADSL o una rete aziendale), poiché in tal caso deve essere egli stesso ad inserire, in un apposito form, nella pagina web del merchant, il proprio numero di telefonia mobile e l'operatore telefonico di riferimento.

Terminata questa fase, il sistema verifica la corretta associazione tra il numero telefonico e l'operatore e reindirizza l'utente su una pagina web del soggetto aggregatore. Contestualmente, l'utente riceve un sms sul numero indicato, contenente un PIN che funge da password ed abilita all'acquisto, una volta inserito in un apposito form presente all'interno della suddetta pagina web. Eseguita tale operazione, l'utente riceve, anche in questo caso, un sms di conferma dell'acquisto. Il descritto processo, che ricade interamente sotto la gestione e la responsabilità dell'aggregatore, consente di verificare il possesso della sim a cui corrisponde il numero telefonico in capo all'utente che sta effettuando l'acquisto e, successivamente, di procedere al controllo della disponibilità del credito telefonico ai fini della fattibilità dell'operazione.

Come si è detto, attraverso la piattaforma abilitante può essere gestito anche un servizio "self care" che permette all'utente la consultazione dello storico degli acquisti effettuati con i diversi merchant e consente, attraverso un'apposita interconnessione realizzata dall'aggregatore, un'analoga interrogazione anche ai customer care degli operatori.

Qualora la piattaforma sia gestita, per aspetti diversi dell'operazione di mobile remote payment (ad esempio reportistica e fatturazione rispetto ad assistenza alla clientela) da più aggregatori, il funzionamento del servizio può implicare un flusso di dati tra database dei differenti hub tecnologici.

Ulteriori interrogazioni tra le banche dati possono essere inoltre previste nel caso in cui sia lo stesso utente ad effettuare la disattivazione del servizio attraverso un cruscotto self care, nonché per verificare il raggiungimento della soglia massima di spesa prevista dalla normativa.

In un quadro così delineato, posto che gli aggregatori operano in tempi differenti, svolgendo funzioni diverse, si ritiene necessario, con specifico riguardo al corretto trattamento dei dati personali, dar conto di due esigenze e prevedere apposite misure di sicurezza.

La prima, legata alla confidenzialità del dato, ovvero alla necessità di garantire che il trasferimento di dati da un soggetto all'altro avvenga secondo elevati standard di sicurezza, implica la cifratura del collegamento.

La seconda esigenza, legata all'accuratezza del dato, implica la necessità che, anche in assenza di un allineamento real time tra le banche dati degli aggregatori, sia l'utente che i customer care degli operatori siano posti sempre nella condizione di "ricostruire lo storico degli acquisti" entro un arco temporale non superiore alle 24 ore.

Inoltre, con riguardo alla verifica delle soglie di spesa relative agli acquisti effettuati dall'utente, gli aggregatori devono porre in essere un sistema di controlli idoneo a garantire un riscontro istantaneo sull'eventuale superamento del tetto previsto.

*7.5. Dati trattati. Misure di sicurezza.*

Le informazioni contenute nella piattaforma gestita dall'aggregatore riguardano normalmente il numero telefonico mobile dell'utente, il codice identificativo del prodotto digitale, la descrizione del prodotto digitale, la data e l'ora dell'operazione di acquisto con il relativo importo, nonché l'esito (positivo-negativo) della stessa. A tali dati si aggiungono, inoltre, quelli che ineriscono alla disattivazione del servizio, nonché tutti gli sms che riguardano la relativa attivazione e disattivazione.

L'aggregatore può inoltre mantenere traccia di tutte le richieste di contenuti/servizi digitali comunque effettuate dai clienti, di tutti i contenuti digitali offerti dai merchant (ovvero direttamente se previsto) con indicazione del relativo destinatario, orario, stato di erogazione, oltre alla classe di costo associata a ciascuno di essi.

Rispetto ai dati contenuti nella piattaforma tecnologica l'aggregatore deve quindi adottare le medesime misure già individuate con riguardo all'operatore, in particolare prevedendo la menzionata procedura di strong authentication degli addetti che hanno accesso alla piattaforma e che devono essere nominati incaricati del trattamento, nonché il tracciamento analitico e dettagliato delle operazioni di accesso, per le quali opera, tuttavia, l'abilitazione tramite l'utilizzo di un'unica chiave di interrogazione del sistema, costituita dal numero di telefonia mobile dell'utente.

Alla luce delle misure individuate rispetto all'attività dell'operatore, con riguardo ai messaggi sull'esito delle transazioni che vengono inviati all'aggregatore, ai fini della necessaria gestione dell'operazione di mobile payment e della successiva attività di reportistica, quest'ultimo deve, nelle proprie tabelle interne di codifica, disporre solo di indicazioni relative a messaggi e codici che non consentano di risalire puntualmente a dati legati alla mancanza od insufficienza di credito telefonico.

*7.6. Conservazione.*

Come già rilevato, i dati personali trattati nell'ambito delle operazioni di mobile remote payment devono essere conservati per un limitato periodo di tempo, proporzionato alle finalità realizzate con il trattamento.

Alla luce di considerazioni del tutto analoghe a quelle già effettuate rispetto all'attività svolta dall'operatore ed alle relative finalità, il periodo massimo di conservazione dei dati trattati dall'aggregatore, ivi compresi gli sms di attivazione e di disattivazione del servizio, è quindi individuato in sei mesi al termine dei quali gli stessi devono essere cancellati dai relativi sistemi.

Resta in ogni caso salva l'ulteriore, specifica, conservazione, necessaria in presenza di una contestazione anche in sede giudiziale.

Ai fini della decorrenza del previsto periodo di conservazione si ritiene inoltre necessario, anche in questo caso, differenziare gli acquisti one shot dagli abbonamenti, posto che per questi ultimi detto periodo deve cominciare a decorrere dalla scadenza dell'abbonamento stesso.

Resta altresì inteso che, laddove l'aggregatore, in veste di titolare del trattamento, effettui attività che, al pari del merchant, implicano l'utilizzo dell'indirizzo IP dell'utente, detto dato dovrà essere immediatamente cancellato dai relativi sistemi una volta conclusa l'operazione di acquisto del contenuto digitale.

**8. Adempimenti del "merchant".**

*8.1. Descrizione dell'attività e modalità di erogazione del servizio.*

Attualmente, nell'ambito del mobile remote payment, i merchant che aderiscono al servizio vendono prodotti editoriali (singole copie del quotidiano o servizi in abbonamento anche in formato digital edition ed e-book), contenuti multimediali in modalità streaming, broadcasting (serie tv e Film) e download, giochi, community e servizi inerenti, nonché servizi relativi a materiale a carattere sessuale.

Il servizio offerto risulta fruibile dal cliente sia da web, sia da dispositivo mobile. Talora, risulta obbligatoria la preventiva registrazione dell'utente al sito web del merchant.

Come si è già evidenziato, attraverso l'uso del personal computer (ricorrendo alla linea ADSL o wireless) i prodotti possono essere acquistati dall'utente collegandosi direttamente al sito del merchant e adottando la procedura già richiamata con riguardo alle modalità di erogazione del servizio nella sezione dedicata al soggetto aggregatore.

Se si utilizzano, invece, dispositivi mobili la procedura prevista per l'attivazione del servizio risulta essere più veloce in quanto, come visto, una volta che l'utente abbia inserito nella pagina web del merchant il numero di telefonia mobile e l'operatore di riferimento è quest'ultimo ad effettuare immediatamente l'associazione tra il terminale mobile ed il numero di telefono.

In alcuni casi l'utente può avvalersi anche di un'opzione "multicanale" che consiste nella possibilità di fruire del contenuto digitale da più terminali. In tale ipotesi l'utente deve effettuare una registrazione al sito del merchant, fornendo anche il proprio indirizzo di posta elettronica che può essere utilizzato da quest'ultimo sia per comunicazioni di servizio, sia come chiave identificativa.

Nel contesto delle suddette operazioni, pertanto, i dati trattati dal merchant risultano essere molteplici e riguardano il numero di telefonia mobile indicato dall'utente all'atto dell'acquisto del contenuto digitale, ovvero comunicato dall'operatore, la data e l'ora dell'operazione, la descrizione del bene acquistato ed il relativo importo, l'identificativo della sessione e l'indirizzo IP, nonché, in alcune ipotesi, l'indirizzo di posta elettronica dell'utente.

*8.2. Informativa.*

Analogamente a quanto già evidenziato, anche nell'informativa che il merchant deve rendere all'utente con riguardo all'acquisto di beni digitali attraverso il ricorso al mobile remote payment, deve risultare chiaro il richiamo sia alla finalità della fornitura del prodotto o servizio, sia alle ulteriori finalità per le quali i dati personali possono essere trattati.

In tale ultima ipotesi l'informativa deve evidenziare tutti i profili già individuati per l'operatore con riguardo ad eventuali attività di profilazione e marketing diretto, programmi di fidelizzazione, nonché trattamenti di comunicazione a terzi e fruizione di contenuti digitali da cui possa dedursi un orientamento dell'utente che implichi un trattamento di dati di natura sensibile.

Nell'informativa deve essere altresì presente il richiamo all'esercizio dei diritti sanciti dall'art. 7 del Codice ed il riferimento ai soggetti eventualmente designati responsabili del trattamento, con particolare riguardo al ruolo che può essere svolto dall'aggregatore, nonché di quelli designati incaricati.

L'informativa del merchant deve inoltre fare espressa menzione del trattamento del dato relativo sia al numero di telefonia mobile dell'utente, sia a quello eventualmente relativo all'indirizzo di posta elettronica, nonché, se effettuato, del trattamento del dato riferibile all'indirizzo IP, specificando che tali informazioni possono essere utilizzate, senza acquisire il consenso dell'utente, solo per finalità di erogazione del contenuto digitale e di migliore e più efficace gestione del servizio.

In ragione dei vincoli di spazio, legati alle dimensioni degli schermi dei terminali anche all'informativa del merchant deve essere data idonea evidenza adottando le medesime modalità già descritte con riguardo al trattamento svolto dall'operatore, in particolare, rispetto al cd. approccio layered.

*8.3. Consenso.*

In veste di titolare autonomo del trattamento il merchant deve acquisire il consenso dell'utente con riguardo a tutti i trattamenti, già individuati rispetto all'operatore eventualmente svolti per finalità di marketing diretto e/o per finalità di profilazione (anche nell'ambito di programmi di fidelizzazione), ovvero di comunicazione dei dati a soggetti terzi, o ancora di fruizione di contenuti digitali da cui possa dedursi un orientamento dell'utente che implichi un trattamento di dati di natura sensibile.

Con riguardo alle modalità di acquisizione del consenso, anche in questo caso, operano tutte le disposizioni già individuate rispetto al

trattamento svolto dall'operatore, nonché tutte le considerazioni espresse dall'Autorità.

*8.4. Dati trattati. Misure di sicurezza.*

Come si è evidenziato, i dati trattati dal merchant nell'ambito delle operazioni di mobile remote payment spaziano dal numero di telefonia mobile dell'utente, all'indirizzo IP sino, eventualmente, al relativo indirizzo di posta elettronica.
Al merchant può essere altresì inviato un messaggio o un codice identificativo della causa della mancata erogazione del servizio da cui, tuttavia, per le considerazioni già svolte rispetto all'operatore, non deve essere possibile risalire alle motivazioni di carattere economico per le quali l'operazione di acquisto non è andata a buon fine.

Conseguentemente, anche il merchant nelle proprie tabelle interne di codifica, deve disporre solo di indicazioni relative a messaggi e codici che non consentano di risalire puntualmente a dati legati alla mancanza od insufficienza di credito telefonico.

La medesima ratio deve essere richiamata con riguardo al livello di profondità e di dettaglio dei dati che il merchant trasmette a propria volta all'operatore, nel senso che le tabelle inviate a quest'ultimo non devono contenere dati immediatamente identificativi dello specifico contenuto digitale acquistato dall'utente, essendo sufficiente la menzione della sola categoria merceologica di appartenenza, o del solo servizio in abbonamento.

Ciò in quanto determinati beni digitali possono risultare idonei a rivelare orientamenti dell'utente che possono implicare un trattamento di dati di natura sensibile, ovvero in quanto le peculiarità stesse dell'attività svolta dal merchant, risultino un chiaro indicatore di gusti e preferenze di consumo dell'utenza. In tal senso idonee misure di sicurezza sono costituite dall'applicazione sull'anagrafica del bene digitale, censito nella banca dati interna del merchant, di un criterio di codificazione del dato, nonché dall'uso di report aggregati da inviare all'operatore.
Rispetto ai dati presenti nel database del merchant ed al relativo accesso da parte dei soggetti addetti al trattamento nell'ambito dell'attività di customer care, valgono tutte le indicazioni già individuate per l'operatore, e, in particolare, la nomina di tali soggetti ad incaricati ai sensi del menzionato art. 30 del Codice, la disponibilità di chiavi di decifrazione dei dati solo rispetto alla suddetta attività di assistenza alla clientela, l'adozione di una procedura di strong authentication ed il tracciamento analitico e dettagliato delle operazioni effettuate, nonché, in questo caso, il ricorso all'utilizzo di una sola chiave di interrogazione del sistema, costituita dal numero di telefonia mobile dell'utente.

Con specifico riguardo al dato costituito dal numero di telefonia mobile dell'utente, posto che il merchant ne dispone nell'ambito della sessione di navigazione al proprio sito per la fase di pagamento immediatamente successiva alla scelta del bene, per eventuali contestazioni in merito alla relativa fruizione, nonché per attività di customer care, occorre evidenziare che il trattamento è ammissibile senza l'acquisizione del consenso dell'utente solo per tali specifiche finalità, proprio in quanto connesse all'erogazione del servizio e alla corretta gestione del medesimo.

Anche il trattamento del dato relativo all'indirizzo di posta elettronica dell'utente, talvolta inserito nella pagina web del merchant, implica analoghe considerazioni.
Tale dato può essere infatti utilizzato per inviare al cliente un messaggio di riscontro dell'avvenuta operazione di acquisto, nonché le istruzioni per accedere al contenuto digitale, consentendo al merchant di gestire meglio il servizio ed il rapporto con l'utente, anche rispetto alla risoluzione di eventuali contestazioni legate alla mancata o insoddisfacente fruizione del bene.

A ciò può aggiungersi la possibilità di garantire all'utente il disaccoppiamento tra il canale di pagamento ed il canale di fruizione del contenuto, consentendogli di pagare il bene digitale attraverso il proprio credito telefonico e di fruirne su qualsiasi altro terminale, in quanto il contenuto acquistato può essere recuperato in qualsiasi momento, accedendo al link indicato nell'e-mail che il merchant invia all'indirizzo di posta elettronica fornito dall'interessato.

Un'ulteriore possibilità offerta è poi quella di arricchire nel tempo il contenuto acquistato attraverso aggiornamenti ed altre informazioni, che non sarebbe altrimenti possibile offrire all'utente se si vincolasse la fruizione del contenuto al terminale con il quale quest'ultimo effettua il pagamento e al momento in cui lo stesso contenuto è scaricato.

In un contesto come quello rappresentato anche l'utilizzo da parte del merchant dell'indirizzo di posta elettronica dell'utente deve essere limitato a tali specifiche finalità e alla migliore e più efficace gestione del servizio.

Anche con riguardo all'eventuale utilizzo dell'indirizzo IP da parte del merchant, deve precisarsi che, se trattato, tale dato deve essere utilizzato esclusivamente ai fini della navigazione dell'utente sul relativo sito, nonché dell'"instradamento" del bene digitale richiesto. I merchant non rientrano, infatti, tra le categorie di soggetti che possono conservare tale dato ai sensi delle citate direttive del Parlamento europeo e del Consiglio 2002/58/CE del 12 luglio 2002 e 2006/24/CE del 15 marzo 2006.

*8.5. Conservazione.*

Con riguardo alla conservazione dei dati personali trattati nell'ambito delle operazioni di mobile payment da parte del merchant anche per quest'ultimo valgono le medesime considerazioni e le conseguenti prescrizioni individuate rispetto all'operatore. Con specifico riguardo all'indirizzo IP dell'utente, tale dato deve, invece, essere immediatamente cancellato dai sistemi del merchant, una volta terminata la procedura di acquisto del contenuto digitale.

*8.6. Notificazione del trattamento.*

Laddove ne ricorrano i presupposti, i trattamenti effettuati nell'ambito delle operazioni di mobile remote payment dovranno essere notificati ai sensi dell'art. 37 del Codice.

*8.7. Richiesta di verifica preliminare.*

Resta altresì inteso che per ulteriori, specifici, trattamenti ed eventuali misure ed accorgimenti, previsti nell'ambito delle operazioni di mobile remote payment diversamente da quanto individuato nel presente provvedimento, sarà necessario presentare al Garante una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, indicando nel dettaglio i trattamenti da effettuare, specificando le relative finalità nonché le tipologie di dati che si intenda utilizzare.

**TUTTO CIÒ PREMESSO, IL GARANTE**

ai sensi dell'art. 154, comma 1, lett. c), del Codice, prescrive a tutti i titolari che effettuato trattamenti di dati personali nell'ambito delle operazioni di mobile remote payment, nel rispetto dei principi generali di liceità, pertinenza, non eccedenza, correttezza e buona fede di cui all'art. 11 del Codice:

A) l'adozione delle misure e degli accorgimenti individuati nel presente provvedimento e specificamente:

1) con riguardo agli adempimenti dell'operatore, ovvero del fornitore di reti e servizi di comunicazione elettronica accessibili al pubblico, tutte le misure indicate ai punti 6.2.; 6.3.; 6.4; 6.5. e 6.6.;

2) con riguardo agli adempimenti del soggetto aggregatore, ovvero del c.d. hub tecnologico, tutte le misure indicate ai punti 7.2.; 7.3.; 7.4.; 7.5. e 7.6.;

3) con riguardo agli adempimenti del merchant, ovvero del fornitore di contenuti digitali, tutte le misure indicate ai punti 8.2.; 8.3.; 8.4. e 8.5.

B) l'adozione delle misure e degli accorgimenti di cui ai precedenti punti entro e non oltre centottanta giorni decorrenti dalla data di pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana;

Avverso il presente provvedimento può essere proposta opposizione ai sensi degli artt. 152 del Codice e 10 del d.lg. n. 150/2011 con ricorso dinanzi all'autorità giudiziaria ordinaria, in particolare al tribunale del luogo ove risiede il titolare del trattamento, da presentarsi entro il termine di trenta giorni dalla data della sua comunicazione ovvero di sessanta giorni se il ricorrente risiede all'estero.

Si dispone la trasmissione di copia del presente provvedimento al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

*Roma, 22 maggio 2014*

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia