CSA Italy

Servizi di pagamento via internet: il contesto normativo italiano per gli aspetti di sicurezza dei dati ed ipotesi di mapping rispetto ai controlli CSA CCM

Ottobre 2015

Sponsor

Introduzione

Il settore dei servizi dei pagamenti effettuati per via informatica/telematica tramite l'utilizzo di computer e terminali mobili presenta anche in Italia caratteristiche di spettacolare crescita, come evidente dall'esperienza di noi tutti nella vita sociale ed in quella professionale e come rilevano diversi osservatori, vedasi ad esempio:

- nel 2014 11 milioni di acquirenti "abituali" hanno comprato su Internet almeno una volta al mese.[...] oltre 200 milioni di transazioni nell'intero 2014 [...] *(dati dalla quarta rilevazione trimestrale di fine gennaio 2015 "Net Retail – Il ruolo del digitale negli acquisti degli italiani", realizzata da Netcomm con il supporto di Human Highway e in partnership con Banzai, Postecom e QVC)*
- "Aumenta l'uso del new digital payment nel 2014: +20% rispetto al 2013 per un controvalore di 18 miliardi di euro " (*www.osservatori.net, Infografica 'Mobile payment non manca più nessuno, 2015)*

ed inevitabilmente si assiste ad un corrispondente eccezionale incremento di casi di frodi/attacchi ai sistemi di pagamento: ad esempio già nel 'lontano 2012' nella SEPA[1] ammontava a 794 millioni di euro la stima delle perdite dovute a 'frodi'(*European Central Bank – February 2014 "THIRD REPORT ON CARD FRAUD")*, e come recentemente riportato dal MEF nel suo report riguardo le frodi sull'uso delle carte di pagamento[2], "*possibile ipotizzare un nuovo modus operandi criminale che predilige la parcellizzazione e la moltiplicazione delle transazioni per aggirare le soglie di attenzione sia degli istituti emittenti sia degli stessi utenti*".

La sicurezza dei dati assume quindi una importanza strategica in questo settore ed a livello di standard vi è grande attenzione nel derivare regolamentazioni e raccomandazioni specifiche come è il caso del PCI Security Standards Councils con le sue recenti pubblicazioni[3].

È però di tutta evidenza l'importanza degli interventi a livello legislativo nello stabilire regole di sicurezza efficaci, adatte in funzione degli specifici mezzi e strumenti di pagamento, tecnologicamente neutre e tali da non creare squilibri tra operatori del settore in base al contesto normativo (nazionale, comunitario, extraeuropeo,...) che sono vincolati ad osservare.

Il tema è dunque assai ampio e si presta ad innummerevoli e complesse analisi che a nostro avviso al momento offrono una limitata stabilità considerando le dinamicità del settore e delle regole con le quali si intende normarlo, anche alla luce di importanti fenomeni quali le Valute Virtuali (un nome su tutti: il Bitcoin) potenzialmente destabilizzanti per l'attuale sistema di governo delle valute e relativi mercati.

Pert tali motivi questo studio condotto da CSA Italy ha ristretto l'attenzione al caso dei pagamenti effettuati via Internet data la loro ampia diffusione presso il pubblico sia in ambito privato che professionale, per i quali a livello normativo comunitario ed italiano esistono già importanti e recenti regole da osservare in materia di sicurezza dei dati, oltre a quelle derivanti dalla normativa in materia di protezione dei dati personali. In questo contesto lo studio intende:

- fornire un quadro riepilogativo di assieme delle norme di sicurezza di legge da tenere presenti e
- proporre un primo mapping verso i controlli individuati da CSA (CSA Corporate https://cloudsecurityalliance.org) con la "CLOUD CONTROLS MATRIX VERSION 3.0.1", delle fondamentali Linee Guida emesse da EBA a fine 2014 in materia di sicurezza nei pagamenti via Internet. Questo mapping potrà successivamente essere raffinato e rivisto concordemente con CSA.

---

[1] Single Euro Payments Area

[2] MEF - Ministero delle economia e delle finanze: "Rapporto statistico sulle frodi con le cartedi pagamento No. 5/2015", http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/antifrode_mezzi_pagamento/antifrode_mezzi_pagamento/Ultimo_Rapporto_Statistico_Carte_di_Pagamento_.pdf. (sito acceduto il 18 Ottobre 2015)

[3] vedasi ad esempio " Accepting Mobile Payments with a Smartphone or Tablet" (https://www.pcisecuritystandards.org/documents/accepting_mobile_payments_with_a_smartphone_or_tablet.pdf)

Indice

Introduzione....3
Si ringrazia....5
1.0 Premessa sui servizi di pagamento via internet....6
2.0 Il contesto normativo in materia di servizi di pagamento....7
2.1 I principali enti di riferimento....7
2.2 Vigenti direttive europee e loro recepimento italiano....10
2.2.1 Le definizioni normative relative ai servizi di pagamento....12
2.3 La futura direttiva PSD 2 ed il ruolo di EBA....15
2.4 Fonti prescrittive in materia di sicurezza nel trattamento dati personali....16
2.4.1 Il Provvedimento del Garante Privacy nel caso di Mobile Remote Payment....17
3.0 La Linea Guida sicurezza EBA/GL/2014/12....18
3.1 Premessa....18
3.2 Contesto di applicabilità....20
3.3 Uno sguardo alla Linea Guida EBA/GL/2014/12....22
3.4 Caso Italia: la consultazione pubblica avviata dalla Banca d'Italia....25
3.5 Mapping delle linee guida sicurezza EBA nei controlli CSA....26
4.0 Nota sulle valute virtuali: fattori di successo e fattori di rischio....28
4.1 Introduzione sulle Valute Virtuali....28
4.2 Il Bitcoin, la VV di maggior successo....30
4.3 I fattori di rischio connaturati alle Valute Virtuali: profili penali....33
5.0 Acronimi....36
6.0 Bibliografia....37

Si ringrazia

Coordinatore del Gruppo di Lavoro "Legal & Privacy in the Cloud"

Gloria Marcoccio

Autori

Gloria Marcoccio

Ettore Corsini

Si ringrazia il dott. Luciano Delli Veneri per il competente ed attento supporto fornito agli Autori nella fase preparatoria dello studio

CSA Staff

Valerio Vertua (coordinatore Comitato Scientifico)

Review

Comitato Scientifico CSA Italy

Consiglio Direttivo CSA Italy

Sponsor

Trend Micro

1.0 Premessa sui servizi di pagamento via internet

I servizi di pagamento basati su sistemi, reti e dispostivi informatici/telematici, da un punto di vista normativo non possono ancora contare su un assetto di definizioni totalmente stabile, definito ed internazionalmente riconosciuto. Per cui ai fini di questo studio è essenziale circoscrivere subito il significato da attribuire ai servizi di pagamento via Internet, chiarendo poi nei successivi paragrafi, dedicati alle norme specifiche comunitarie e nazionali, i relativi legami con le definizioni di legge.

Per 'servizi di pagamento via Internet', indipedentemente dal tipo di dispositivo utilizzato per effettuare un acquisto (computer, smartphone,...), qui si intendono inclusi i seguenti

A. [Carte] esecuzione dei pagamenti con carta su internet, compresi i pagamenti con carte virtuali, così come la registrazione dei dati di carte di pagamento per l'utilizzo con mediante soluzioni di portafoglio elettronico
B. [Bonifici] l'esecuzione dei bonifici (Credit Transfers) su Internet
C. [E-mandato] l'emissione e la modifica dei mandati elettronici di addebito diretto
D. [E-money] trasferimenti di moneta elettronica tra due conti di moneta elettronica via Internet

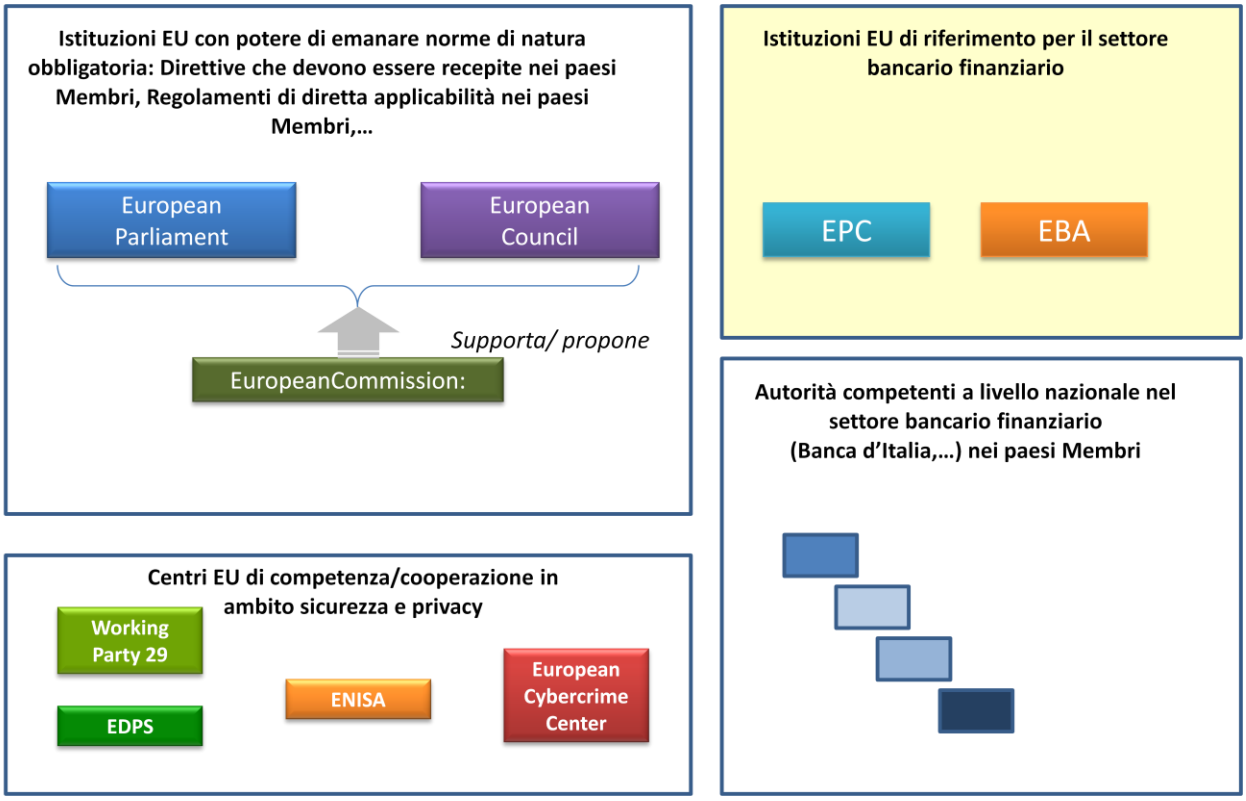
esclusi i seguenti:

I. Altri servizi internet forniti da un PSP (Payment Service Provider ossia i Fornitori di Servizi di Pagamento) tramite il suo sito web di pagamento (ad esempio e-intermediazione, contratti on-line)
II. I pagamenti in cui l'istruzione è data per posta, per telefono, posta vocale o utilizzando la tecnologia basata su SMS (Short Message Service)
III. Pagamenti effettuati da terminale mobile diversi dai pagamenti basati su browser
IV. Credit Transfer in cui un terzo accede al conto di pagamento del cliente
V. Operazioni di pagamento effettuate da un'impresa tramite reti dedicate

Questa delimitazione di significato è esattamente quella identificata nella Linea Guida EBA/GL/2014/12 in materia di sicurezza nei pagamenti Internet, commentata nei successivi paragrafi.

2.0 Il contesto normativo in materia di servizi di pagamento

2.1 I principali enti di riferimento



La normativa comunitaria è prodotta dal **Parlamento Europeo** e dal **Consiglio Europeo** tipicamente su proposta della **Commissione Europea.**

L'**European Cybercrime Centre- EC3**[4], ospitato presso l'Europol[5], attivo a partire dal Gennaio 2013, ha il compito di agire come *focalpoint* nella lotta EU contro il *cyber crime* contribuendo a velocizzare le reazioni in caso di crimini commessi *on line* e inoltre ha il compito di supportare gli Stati Membri e le istituzioni dell'Unione Europea nel realizzare capacità operative e di analisi per attività investigative ed cooperazioni internazionali.

ENISA[6] è invece l'agenzia europea con il ruolo di centro di competenza EU per la sicurezza delle reti e dell'informazione, istituita a partire dal 2004 per migliorare la capacità della Unione Europea, degli Stati Membri e la comunità del business nel prevenire, indirizzare e rispondere a problematiche inerenti appunto la sicurezza

[4] https://www.europol.europa.eu/ec3
[5] http://www.europol.europa.eu/
[6] http://www.enisa.europa.eu/

delle reti e delle informazioni. Sullo scenario internazionale ENISA può essere paragonata, sul piano degli intenti, al centro di competenza statunitense NIST[7].

Occorre poi menzionare il **Working Party 29**[8], consesso dei garanti privacy[9] degli Stati Membri EU, istituito tramite appunto l'articolo 29 della vigente direttiva europea 95/46/EC relativa alla protezione dati personali e privacy, che ha il compito di assistere le istituzioni europee in tale materia. Sebbene non sia un organismo dotato di poteri decisionali, ha comunque una grande influenza sulla impostazione della normativa in questione e di conseguenza sui provvedimenti emanati a livello di singolo stato Membro proprio perché il WP 29 è formato dalle autorità nazionali competenti per la privacy e protezione dati personali.

Infine occorre citare l'**European Data Protection Supervisor (EDPS)**[10] autorità indipendente Europea il cui principale obiettivo è assicurare che le istituzioni e gli enti Europei rispettino il diritto alla privacy e alla protezione dei dati personali nel trattamento dei dati per loro finalità e scopi e nello sviluppo di nuove politiche. L'EDPS opera in base alla apposita Regulation 45/2001, ed è presieduto attualmente da Giovanni Buttarelli.

Sul versante degli standard internazionali e dunque di quelle normative che, pur non avendo la forza di un obbligo di legge, di fatto stabiliscono requisiti essenziali e di riferimento per il business, occorre senz'altro tenere presente l'ente **ISO** (International Organization for Standardization)[11].

[7] http://www.nist.gov/index.html
[8] http://ec.europa.eu/justice/data-protection/article-29/index_en.htm
[9] Dizione correntemente utilizzata per denotare in breve le autorità garanti per la protezione dei dati personali, istituite con la direttiva europea 95/46/CE
[10] http://www.edps.europa.eu/EDPSWEB/
[11] http://www.iso.org/iso/home.html

Specificamente per il settore dei pagamenti hanno poi particolare rilevanza:

- **EPC - European Payment Council -** http://www.europeanpaymentscouncil.eu/index.cfm - È l'ente di coordinamento e decisionale nel contesto SEPA. Supporta e promuove la cooperazione nel settore dei servizi di pagamento, fornisce assistenza nei processi di standardizzazione, formula *best practices,* supporta e monitora affinché le decisioni siano effettivamente prese.
- **EBA - European Banking Authority -** http://www.eba.europa.eu/ - Autorità indipendente dell'Unione europea che opera per assicurare un livello di regolamentazione e di vigilanza prudenziale efficace e uniforme nel settore bancario europeo.

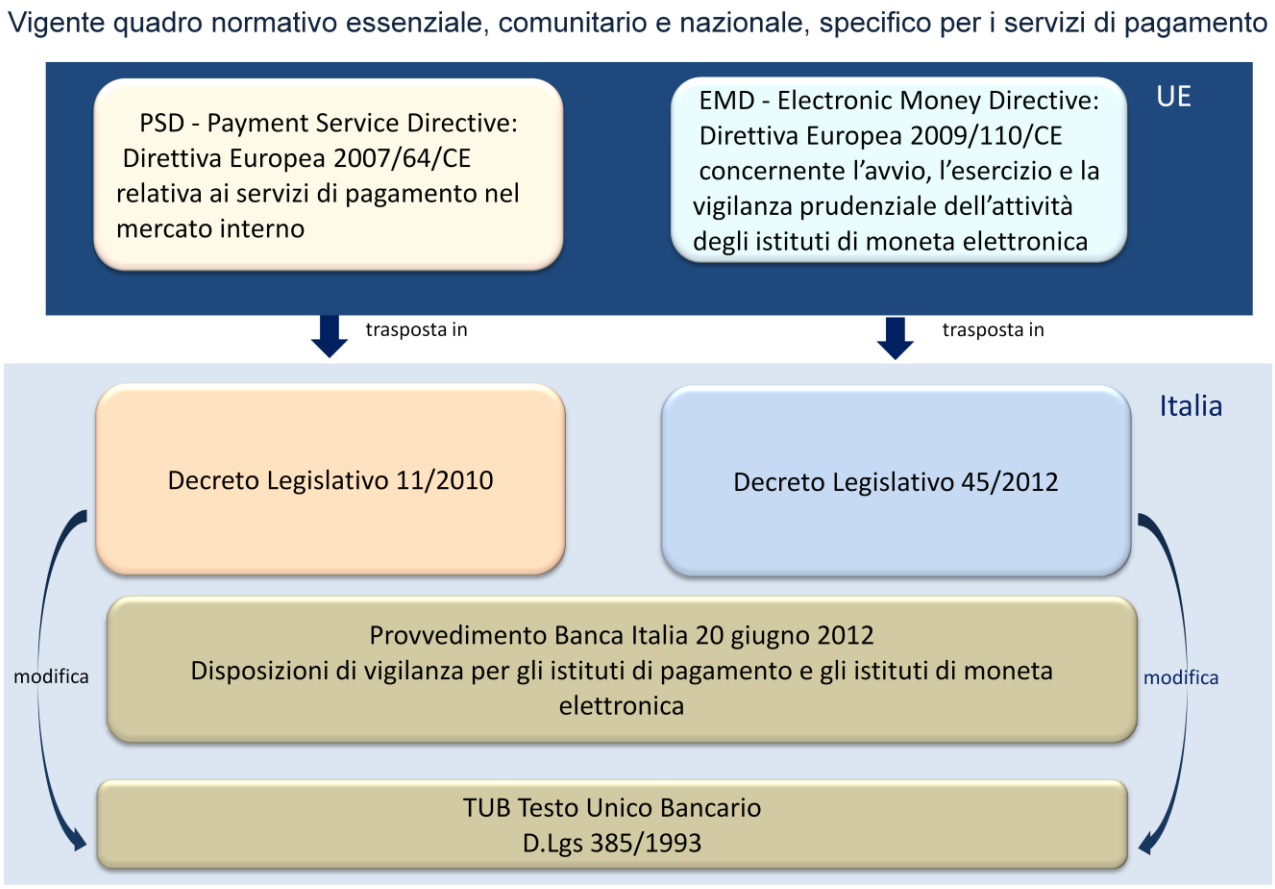
Gli obiettivi generali dell'Autorità sono assicurare la stabilità finanziaria nell'UE e garantire l'integrità, l'efficienza e il regolare funzionamento del settore bancario

Il compito principale è contribuire, **attraverso l'adozione di norme tecniche vincolanti e orientamenti**, alla creazione del corpus unico di norme del settore bancario che consentano di assicurare condizioni di parità e una tutela elevata dei depositanti, degli investitori e dei consumatori

È stata istituita nel 2010 con apposito Regolamento Europeo n. 1093/2010 che ne fissa ruoli e responsabilità. Questa autorità ha ed avrà sempre più un ruolo centrale e strategico nel determinare le misure di sicurezza rilevanti ai fini delle leggi comunitarie relativamente ai pagamenti: nella prossima direttiva PSD 2 (seconda Direttiva sui Servizi di Pagamento che abrogherà e sostituirà totalmente l'attuale PSD 1 2007/64/CE, vedasi successivi paragrafi) gli è in tal senso assegnato il ruolo primario.

A livello poi di singolo paese membro UE vi sono le corrispondenti autorità nazionali (nel nostro caso: la Banca d'Italia) che nel settore finanziario/bancario predispongono ed attuano le regolamentazioni nazionali in coordinamento/recepimento con le applicabili leggi e regolamenti comunitari.

2.2 Vigenti direttive europee e loro recepimento italiano



Qui di seguito sono riportate in modo sintetico le principali caratteristiche della normativa in oggetto, per quanto di interesse ai fini dello studio, centrato sulle misure di sicurezza.

Direttiva PSD:

- Si applica ai servizi di pagamento prestati nella Comunità Europea
- Identifica quali servizi sono inclusi/esclusi
- Identifica le categorie di prestatori di servizi di pagamento
- Stabilisce le regole da osservare per il processo autorizzativo da applicare ad un istituto di pagamento a cura delle autorità competenti dei paesi membri UE
- Non include specifiche prescrizioni in materia di sicurezza
- Nei prossimi due/tre anni sarà totalmente sostituita dalla nuova direttiva già denominata PSD2 (vedasi apposito paragrafo seguente)

D.Lgs 11/2010, di recepimento della Direttiva PSD:

- Modifica il TUB (Testo Unico Bancario) in particolare per quanto riguarda il processo autorizzativo degli Istituti di pagamento, a cura della Banca d'Italia
- Non include specifiche prescrizioni in materia di sicurezza
- Vi è un esplicito riferimento alla normativa protezione dati personali per quanto riguarda la gestione frodi:

> *Art. 29 Protezione dei dati*
>
> *1. I prestatori di servizi di pagamento e i gestori di sistemi di pagamento possono trattare dati personali ove cio' sia necessario a prevenire, individuare e indagare casi di frode nei pagamenti. Il trattamento avviene in conformita' al decreto legislativo 30 giugno 2003, n. 196.*

Direttiva EMD:

- Fissa norme per l'esercizio dell'attività di emissione di moneta elettronica nel contesto della comunità europea
- Identifica le categorie di emittenti di moneta elettronica
- Riconosce l'applicabilità della direttiva PSD agli istituti emittenti moneta elettronica
- Stabilisce le regole da osservare per il processo autorizzativo da applicare ad un emittente di moneta elettronica (da parte delle autorità competenti nei paesi membri UE)
- Non include specifiche prescrizioni in materia di sicurezza

D.Lgs 45/2012 di recepimento della Direttiva EMD:

- Modifica il TUB in particolare per quanto riguarda il processo autorizzativo degli Istituti emittenti di moneta elettronica (IMEL), a cura della Banca d'Italia
- Non include specifiche prescrizioni in materia di sicurezza

Provvedimento Banca Italia 20 giugno 2012 - Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica

- Stabilisce le procedure da seguire a cura della Banca d'Italia per la gestione del ciclo di vita dei processi di autorizzazione e di vigilanza sugli istituti di pagamento e gli istituti di moneta elettronica
- Per quanto concerne la sicurezza richiesta agli istituti, esiste un riferimento, ma di carattere meramente generale, nell' "Allegato A Ruolo degli organi aziendali, sistemi informativi e sistema dei controlli interni."
- La Banca d' Italia mantiene aggiornati gli elenchi degli istituti di pagamento e di moneta elettronica autorizzati: http://www.bancaditalia.it/compiti/vigilanza/albi-elenchi/

Il ruolo del sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese (SPID)

Il sistema **SPID** è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia Digitale (AGID), gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni. Il 28 luglio 2015, con la Determinazione AGID n. 44/2015 sono stati emanati i quattro regolamenti previsti dall'articolo 4, commi 2, 3 e 4, del DPCM 24 ottobre 2014[12], che riguardano:

1. regole tecniche;
2. modalità attuative per la realizzazione dello SPID
3. modalità di accreditamento dei soggetti SPID;
4. procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale.

Con l'emanazione di tali regolamenti il Sistema Pubblico di Identità Digitale si avvia quindi verso la sua operatività e come tale potrà fornire base per l'autenticazione dei soggetti che effettuano pagamenti quanto meno verso le pubbliche amministrazioni.

2.2.1 Le definizioni normative relative ai servizi di pagamento

Per quanto concerne l'Italia, la normativa nazionale prima riepilogata recepisce in modo totale le definizioni di legge presenti nelle direttive PSD ed EMD, ed in particolare ai fini di questo studio è importante tenere presenti queste definizioni:

Servizi di pagamento *- D.Lgs 11/2010, art 1 lettera b)*

1) *servizi che permettono di depositare il contante su un conto di pagamento nonche' tutte le operazioni richieste per la gestione di un conto di pagamento;*
2) *servizi che permettono prelievi in contante da un conto di pagamento nonche' tutte le operazioni richieste per la gestione di un conto di pagamento;*
3) *esecuzione di ordini di pagamento, incluso il trasferimento di fondi, su un conto di pagamento presso il prestatore di servizi di pagamento dell'utilizzatore o presso un altro prestatore di servizi di pagamento:*
    - *3.1 esecuzione di addebiti diretti, inclusi addebiti diretti una tantum;*
    - *3.2.esecuzione di operazioni di pagamento mediante carte di pagamento o dispositivi analoghi;*
    - *3.3. esecuzione di bonifici, inclusi ordini permanenti;*
4) *Esecuzione di operazioni di pagamento quando i fondi rientrano in una linea di credito accordata ad un utilizzatore di servizi di pagamento:*

[12] Il DPCM "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese." Pubblicato sulla GU Serie Generale n.285 del 9 dicembre 2014

4.1. esecuzione di addebiti diretti, inclusi addebiti diretti una tantum;

4.2. esecuzione di operazioni di pagamento mediante carte di pagamento o dispositivi analoghi;

4.3. esecuzione di bonifici, inclusi ordini permanenti;

5) *emissione e/o acquisizione di strumenti di pagamento;*
6) *rimessa di denaro;*
7) *esecuzione di operazioni di pagamento ove il consenso del pagatore ad eseguire l'operazione di pagamento sia dato mediante un dispositivo di telecomunicazione, digitale o informatico e il pagamento sia effettuato all'operatore del sistema o della rete di telecomunicazioni o digitale o informatica che* ***agisce esclusivamente come intermediario tra l'utilizzatore di servizi di pagamento e il fornitore di beni e servizi****.*

Nota di commento - da notare in particolare al punto 7) la specifica che riguarda il ruolo di solo intermediario dall'operatore del sistema o della rete di telecomunicazioni o digitale o informatica: se tale operatore ha invece un ruolo di diretto coinvolgimento attivo, quale ad esempio di erogatore del bene/servizio acquisito o di gestione acquisto tramite traffico telefonico, allora non siamo in presenza di **Servizi di pagamento** per cui la direttiva PSD non si applica e dunque l'operatore non dovrà sottostare al processo autorizzativo come Prestatore di servizi di pagamento, a cura della Banca d'Italia

Casi esclusi dall'applicazione del provvedimento - D.Lgs 11/2010, art 2 comma 2

a) *operazioni di pagamento effettuate esclusivamente in contante direttamente dal pagatore al beneficiario, senza alcuna intermediazione;*
b) *operazioni di pagamento dal pagatore al beneficiario effettuate tramite un agente commerciale autorizzato a negoziare o a concludere la vendita o l'acquisto di beni o servizi per conto del pagatore o del beneficiario;*
c) *trasporto materiale, a titolo professionale, di banconote e monete, ivi compresa la raccolta, il trattamento e la consegna;*
d) *operazioni di pagamento consistenti nella raccolta e nella consegna di contante, a titolo non professionale, nel quadro di un'attivita' senza scopo di lucro o a fini di beneficenza;*
e) *servizi in cui il beneficiario fornisce contante al pagatore nel contesto di un'operazione di pagamento, a seguito di una richiesta esplicita del pagatore di servizi di pagamento immediatamente precedente l'esecuzione dell'operazione di pagamento attraverso un pagamento destinato all'acquisto di beni o servizi;*
f) *operazioni di cambio di valuta contante contro contante nell'ambito delle quali i fondi non sono detenuti su un conto di pagamento;*
g) *operazioni di pagamento basate su uno dei seguenti tipi di documenti cartacei, con i quali viene ordinato al prestatore di servizi di pagamento di mettere dei fondi a disposizione del beneficiario: assegni, titoli cambiari, voucher, traveller's cheque, vaglia postali;*
h) *operazioni di pagamento realizzate all'interno di un sistema di pagamento o di un sistema di regolamento dei titoli tra agenti di regolamento, controparti centrali, stanze di compensazione e/o banche centrali e altri partecipanti al sistema e prestatori di servizi di pagamento, fatto salvo l'articolo 30;*

i) operazioni di pagamento collegate all'amministrazione degli strumenti finanziari, compresi i dividendi, le entrate o altre distribuzioni, o ai rimborsi o proventi di cessioni, effettuate dalle persone di cui alla lettera h), ovvero da imprese di investimento, enti creditizi, organismi di investimento collettivo o societa' di gestione patrimoniale che prestano servizi di investimento ed ogni altra entita' autorizzata ad avere la custodia di strumenti finanziari;

j) servizi forniti dai prestatori di servizi tecnici, che supportano la prestazione dei servizi di pagamento, ***senza mai entrare in possesso dei fondi da trasferire****, compresi l'elaborazione e la registrazione di dati, i* ***servizi fiduciari e di protezione dei dati personali,*** *l'autenticazione dei dati e delle entita', la fornitura di reti informatiche e di comunicazione, la fornitura e la manutenzione di terminali e dispositivi utilizzati per i servizi di pagamento;*

k) servizi basati su strumenti che possono essere utilizzati per acquistare beni o servizi solo nella sede utilizzata dall'emittente ***o in base ad un accordo commerciale con l'emittente, all'interno di una rete limitata di prestatori di servizi o per una gamma limitata di beni o servizi****; [non costituisce moneta elettronica D.Lgs 45/2012 art. 1 comma 2]*

l) operazioni di pagamento eseguite tramite qualsiasi dispositivo di telecomunicazione, digitale o informatico, ***quando i beni o servizi acquistati sono consegnati al dispositivo*** *di telecomunicazione, digitale o informatico, o devono essere utilizzati tramite tale dispositivo, a condizione che l'operatore di telecomunicazione, digitale o informatico,* ***non agisca esclusivamente quale intermediario tra l'utilizzatore di servizi di pagamento e il fornitore dei beni e servizi;***

m) operazioni di pagamento realizzate tra prestatori di servizi di pagamento, relativi agenti o succursali per proprio conto;

n) *operazioni di pagamento tra un'impresa madre e la relativa filiazione, o tra filiazioni della stessa impresa madre, senza alcuna intermediazione da parte di un prestatore di servizi di pagamento diverso da una delle imprese appartenenti al medesimo gruppo;*

o) *servizi, forniti da prestatori, di prelievo di contante tramite sportelli automatici per conto di uno o piu' emittenti della carta, che non sono parti del contratto quadro con il cliente che preleva denaro da un conto di pagamento, a condizione che detti prestatori non gestiscano altri servizi di pagamento elencati nell'articolo 1.*

Nota di commento - La complessità e criticità della materia e dunque la consapevolezza da parte del legislatore di dover trattare con estrema attenzione il tema dell'applicabilità o meno delle prescrizioni PSD, si evidenzia chiaramente con questa dichiarazione analitica di quali servizi/operazioni risultano essere non in scopo. Interessante notare il punto l) con il quale si chiarisce l'esclusione di servizi tecnici, ancillari e di supporto per i servizi di pagamento (gestioni operative dei sistemi, servizi di firma digitale/trust eventualmente utilizzati nell'operatività di un servizio di pagamento,...). Il punto m) è anch'esso interessante in quanto esclude l'applicabilità della legge in oggetto al caso dei 'gruppi chiusi' di gestione acquisti (circuiti nei quali gli aderenti comprano o vendono beni/servizi in base a determinate regole interne che in genere limitano il ricorso a contante, tipicamente di natura locale in quanto indirizzati a favorire vendite/acquisiti di beni e servizi prodotti localmente). Il punto n) è invece da leggere in relazione al caso di esclusione di operatori di di telefonia quando in un servizio di pagamento svolgono anche dei ruoli attivi (come ad esempio quello di consegnare/rendere

fruibile il bene servizio digitale presso il dispotivo tramite il quale è stato avviato dal cliente il processo di acquisto)

PSP- Prestatori di Servizi di Pagamento - D.Lgs 11/2010, art 1 lettera g)

Uno dei seguenti organismi: istituti di moneta elettronica e ***istituti di pagamento*** *nonche', quando prestano servizi di pagamento, banche, Poste Italiane s.p.a., la Banca centrale europea e le banche centrali nazionali se non agiscono in veste di autorita' monetarie, altre autorita' pubbliche, le pubbliche amministrazioni statali, regionali e locali se non agiscono in veste di autorita' pubbliche;*

Nota di commento - Gli istituti di pagamento sono definiti 'per difetto' e dunque sono quegli istituti che:

- **prestano uno o più dei servizi di pagamento ricompresi nel campo di applicazione della PSD - dunque i servizi di pagamento elencati alla lettera b) art 1 D.Lgs 11/2010**
- **sono diversi da istituti di moneta elettronica nonché banche…..[come elencato alla lettera g) D.Lgs 11/2010]**

La moneta elettronica - D.Lgs 45/2012, art 1 comma 2 che modifica il TUB art. 1 comma 2 lettera h-ter

il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente [della moneta elettronica] che sia emesso per effettuare operazioni di pagamento come definite all'articolo 1, comma 1, lettera c), del decreto legislativo 27 gennaio 2010, n. 11, e che sia accettato da persone fisiche e giuridiche diverse dall'emittente.

Non costituisce moneta elettronica:

1) *il valore monetario memorizzato sugli strumenti previsti dall'articolo 2, comma 2, lettera m), del decreto legislativo 27 gennaio 2010, n. 11* [all'interno di una rete limitata di prestatori di servizi o per una gamma limitata di beni o servizi]
2) *il valore monetario utilizzato per le operazioni di pagamento previste dall'articolo 2, comma 2, lettera n), del decreto legislativo 27 gennaio 2010, n. 11."* [tramite qualsiasi dispositivo di telecomunicazione… operatore TLC che agisce non solo come intermediario]

2.3 La futura direttiva PSD 2 ed il ruolo di EBA

A partire dal 2013 la Commissione Europea ha presentato la proposta di una nuova direttiva riguardo il settore dei pagamenti con particolare attenzione per migliorarne la sicurezza, ampliare le possibilità di scelte per i consumatori e mantenere il passo con le innovazioni tecnologiche che riguardano la materia. Il 5 Maggio di quest'anno la Commissione Europea, il Parlamento Europeo ed il Consiglio d'Europa hanno raggiunto l'accordo

sul testo definitivo della direttiva, a parte alcuni dettagli tecnici che dovrebbero a breve essere anch'essi completamente chiariti. Si prevede quindi che la nuova direttiva PSD2, che abrogherà e sostituirà l'attuale PSD, possa essere definitivamente approvata entro quest'anno. I paesi membri UE dovranno quindi implementare la direttiva PSD 2 presumibilmente entro Ottobre 2017.

La nuova Direttiva PSD2 stabilisce che EBA dovrà definire i requisiti per migliorare la sicurezza negli aspetti operativi dei servizi di pagamento, in stretta cooperazione con la Banca Centrale Europea (ECB).

Considerando gli aspetti temporali, è ritenuto assai improbabile che i requisiti di sicurezza da definire a cura di EBA in contesto PSD2 possano entrare in vigore prima del 2018/2019, per cui anche per questo motivo assume ulteriore notevole importanza la Linea Guida EBA/GL/2014/12 sui pagamenti via Internet, pubblicata il 18 Dicembre 2014, entrata definitivamente in vigore a partire dal primo Agosto 2015, e che tale rimarrà fino a quando non entreranno a loro volta in vigore i requisiti di sicurezza PSD2.

2.4 Fonti prescrittive in materia di sicurezza nel trattamento dati personali

Al caso dei servizi di pagamenti via Internet così come definiti per lo scopo di questo studio (ai quali si applica la Linea Guida EBA/2014/12), nella misura in cui comportanto trattamento di dati personali, si applicano le misure di sicurezza previste dal D.Lgs 196/03 e da determinati Provvedimenti prescrittivi del Garante Privacy. In termini riepilogativi occorre in tal senso tenere presenti:

in ogni caso

- le prescrizioni sulla minimizzaione dei dati ed il rispetto del principio di pertinenza e non eccedenza, inclusa la conservazione dei dati personali solo per il tempo strettamente necessario al perseguimento delle finalità del trattamento dei dati personali (art 3 ed 11 del D.Lgs 196/03 [1])
- le Misure Minime di Sicurezza di cui all'Allegato B del D.Lgs 196/03 [2] (previste sanzioni di natura penale in caso di inosservanza)
- le misure commensurate ai rischi specifici ex art 31 D.Lgs 196/03 [1], quest'ultime da determinare a seguito di apposita analisi dei rischi
- il Provvedimento riguardo la figura dell'Amministratore di Sistema [3]

laddove il servizio comporti il trattamento nel contesto di un servizio di comunicazioni elettrocniche accessibile al pubblico

- apposite misure commensurate al rischio (art 32 D.Lgs 196/03)
- le prescrizioni in caso di violazione dei dati personali (incluse le notifica al Garante privacy e in determinati casi anche notifiche ai soggetti interessati dalle violazioni avvenute, art 32-bis D.Lgs 196/03 [1] e Provvedimento in materia di Data Breach [4])
- le applicabili misure di sicurezza previste dal Provedimento sulla sicurezza dei dati di traffico [5]

laddove il servizio comporti trattamento di dati biometrici (nel caso di utilizzo di strong authentication basata sui dati biometrici)

- il Provvedimento in materia di biometria [6]

2.4.1 Il Provvedimento del Garante Privacy nel caso di Mobile Remote Payment

Sebbene NON riguardi i servizi di pagamento via Internet così come definiti per lo scopo di questo studio (ai quali si applica la Linea Guida EBA/2014/12), è comunque importante qui ricordare che l'Autorità italiana per la protezione dei dati personali (Garante Privacy) ha emesso un recente provvedimento prescrittivo in materia di pagamenti quando operati in questo contesto (condizioni in logica AND):

- effettuati da remoto tramite dispositivo mobile/computer
- nel caso di pagamento effettuato tramite decurtazione del costo dal credito telefonico (pre-pagato) o addebito sul conto telefonico
- con valore di singolo acquisto inferiore a 15 euro,
- quando il bene/servizio acquistato è digitale ed è consegnato/fruito direttamente tramite il dispostivo (es. acquisto di un un filmato visibile direttamente tramute smartphone).

Si tratta del "Provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di mobile remote payment - 22 maggio 2014", pubblicato in Gazzetta Ufficiale n. 137 del 16 giugno 2014.

Le prescrizioni del provvedimento sono entrate definitivamente in vigore a partIre dal 1 Aprile 2015 ed interessano le società che operano nel settore del mobile payment quali le compagnie telefoniche che forniscono il servizio di pagamento tramite cellulare, le società che forniscono l'interfaccia tecnologica, le aziende che offrono contenuti digitali e servizi, nonché tutti gli altri soggetti coinvolti nella transazione (come quelli che consentono, anche tramite app, l'accesso al mercato digitale).

Il Provvedimento prescrive tra l'altro misure di sicurezza per garantire la riservatezza delle persone e impedire l'integrazione delle diverse tipologie di dati a disposizione dell'operatore telefonico (dal consumo telefonico ai dati sul consumo di beni digitali) per fini di profilazione "incrociata" dell'utenza a meno che non venga espresso uno specifico consenso informato dell'utente. Le misure sono specificate in modo diversificato per i ruoli operativi individuati dal Garante Privacy (Operatore telefonico, Aggregatore, Merchant) ed in termini meramente riepilogativi richiedono, oltre alle dovute gestioni dell'Informativa e del Consenso:

- apposite codifiche e forme di mascheramento in relazione ai beni/servizi digitali acquistati come per l'eventuale esito negativo di acquisto per mancanza di fondi (in termini di traffico telefonico)
- tecniche di autenticazione per i preposti (incaricati al trattamento) basate su *strong authentication* e gestione del log delle operazioni effettuate da proposti in relazione al servizio di pagamento

- limiti alla possibilità di 'incrociare' i dati relativi ai beni/servizi digitali acquistati con altri dati ai fini di profilazione
- conservazione dei dati relativi agli acquisiti per untempo non superiore ai 6 mesi dalla data dell'evento/acquisto del contenuto digitale, nel caso di "abbonamento" al servizio/contenuto i 6 mesi decorrono dalla sua cessazione
- applicazione della disciplina in materia di violazione dei dati personali (ai sensi dell'art 32 bis del D.Lgs 196/03) che per tali eventi richiede la Notifica al Garante privacy ed, in alcuni casi, anche ai diretti Interessati.

3.0 La Linea Guida sicurezza EBA/GL/2014/12

3.1 Premessa

EBA ha pubblicato nel Dicembre 2014 la Linea Guida in materia di sicurezza dei pagamenti via Internet, basata su precedenti raccomandazioni realizzate dal European Forum on the Security of Retail Payments (SecuRe Pay) ed a seguito di apposita consultazione condotta sempre nel 2014, alla quale hanno presentato risposte i principali gruppi internazionali attivi nel settore dei servizi di pagamento.

La conversione delle precedenti raccomandazioni in linea guida emesse da EBA fornisce una solida base legale per una implementazione dei relativi requisiti di sicurezza in modo consistente tra i 28 paesi membri UE, rispondendo alla necessità di disporre di un quadro di riferimento per le misure di sicurezza in oggetto che sia subito considerato vigente, senza poter attendere i tempi di pubblicazione e di avvio di vigenza della prossima direttiva PSD2 nella quale la sicurezza nei servizi di pagamentti assume un ruolo fondamentale.

La Linea Guida EBA richiede che le relative misure di sicurezza siano implementate a partire dal 1 agosto 2015.

Per quanto concerne la loro obbligatorietà occorre considerare che la Linea Guida EBA è rivolta alle autorità nazionali (Banca d'Italia per il caso Italiano) le quali sono obbligate, a norma dei regolamenti EBA, a dichiarare se intendono o meno conformarsi agli orientamenti di EBA così definiti e, dunque, rendere le Linee Guida nella concreta sostanza applicabili ai fornitori di servizi di pagamento che operano sul territorio nazionale. Ad oggi, in base alle informazioni pubblicate da EBA [7], il quadro a livello dei paesi membri UE è il seguente.

Tutti i paesi (osssia le relative autorità nazionali competenti) hanno dichiarato di voler procedere in conformità alle Linea Guida in oggetto, con i pochi seguenti casi di esclusione (e relative motivazioni):

Tabella 1 - Quadro di adesione dei paesi membri EU alla Linea Guida EBA/GL/2014/12

Paesi che hanno dichiarato di voler procedere con una PARZIALE conformità rispetto le EBA/GL/2014/12	Paesi che hanno dichiarato di NON VOLER procedere con la conformità rispetto le EBA/GL/2014/12
Cipro *"The Central Bank of Cyprus (CBC) reported that it will comply with all Guidelines, except Guidelines 7.3, 8.1[cards], and 8.2. CBC is therefore partially compliant. CBC also indicated that it intends to be fully compliant without exceptions by 1 August 2016. One month beforehand, the EBA will request confirmation of the notification that the CBC has submitted today and will update the table as appropriate."*	**Estonia** *" The Estonian Financial Supervision Authority (FSA) reported that, in order to implement the final EBA Guidelines on the security of internet payments (EBA/GL/2014/12), Estonian law would need to be changed, but that the FSA lacks legal powers to do so. The FSA is therefore not compliant. FSA indicated that it has approached relevant national ministries and other authorities for analysis and decision. The EBA will review the compliance status as and when national legislation will have changed."*
Svezia *" The Swedish Financial Supervisory Authority reported that it will comply with all Guidelines, except Guidelines 7.6 and 7.7 in respect of payment institutions."*	**Slovakia** *" National Bank of Slovakia (NBS) reported that it cannot cover the GL under its current legal framework. NBS is therefore not compliant."*
	Inghilterra " *FCA reported that it does not have the power without legislative change to make binding rules requiring all payment service providers (credit institutions, payment institutions and e-money institutions) to comply with the EBA Guidelines. The FCA is therefore not compliant. FCA also reported that it has considered what other steps it might take short of making binding rules, including issuing guidance to payment service providers, in the light of its statutory objectives and obligations and its public law duties, and in particular the requirement that FCA has regard to the principle of proportionality (see section 3B(1)(b) of FSMA 2000). It reported that the choreography of the EBA Guidelines and PSD2 is an important aspect of the proportionality analysis. FCA concluded that implementation of the Guidelines will require some providers to make significant changes to their systems and controls and significant additional changes are likely to be necessary following implementation of PSD2. The FCA continued that it had indicated to the UK market in March 2014 that it would be requiring compliance with the SecuRe Pay Recommendations in line with PSD2 transposition requirements. FCA remains of the view that it is reasonable, in all the circumstances, for FCA to incorporate the detail of the Guidelines (or equivalent guidelines issued under PSD2) into its supervisory framework in line with this timetable. FCA's intention is that this will be done in a way that is equally binding on all types of payment service provider. FCA also reported that it is fully supportive of the objectives behind the EBA Guidelines and agrees with the importance of consumers being protected against fraud when making payments online. Ensuring the security of payments and the protection of sensitive customer data is a critical part of the infrastructure of robust payment systems, and FCA has reminded payment service providers of their responsibility to ensure consumers' payments are safe and secure."*

Considerando che EBA dovrà, in base alle prossima direttiva PSD2, definire i requisiti per le misure di sicurezza nei servizi di pagamento, è ben evidente che le attuali Linea Guida rappresentano il set già definito per tali

requisiti nel contesto dei pagamenti via Internet, che potranno essere oggetto di aggiornamenti ed ampliamenti ma non certo di significative variazioni.

Pertanto l' attuale Linea Guida rappresenta un fondamentale riferimento per le misure di sicurezza nei servzi di pagamento via Internet:

- attualmente in quanto il 90% circa dei paesi UE hanno dichiarato di voler procedere in conformità ad esse, fino a quando non saranno vigenti le misure di sicurezza che saranno richieste con la PSD2
- nel prossimo futuro, a partire dal 2018/19 quando la PSD2 sarà definitivamente in vigore.

3.2 Contesto di applicabilità

I servizi di pagamento via Internet in scopo della Linea Guida EBA/GL/2014/12 sono riepilogati nella successiva tabella.

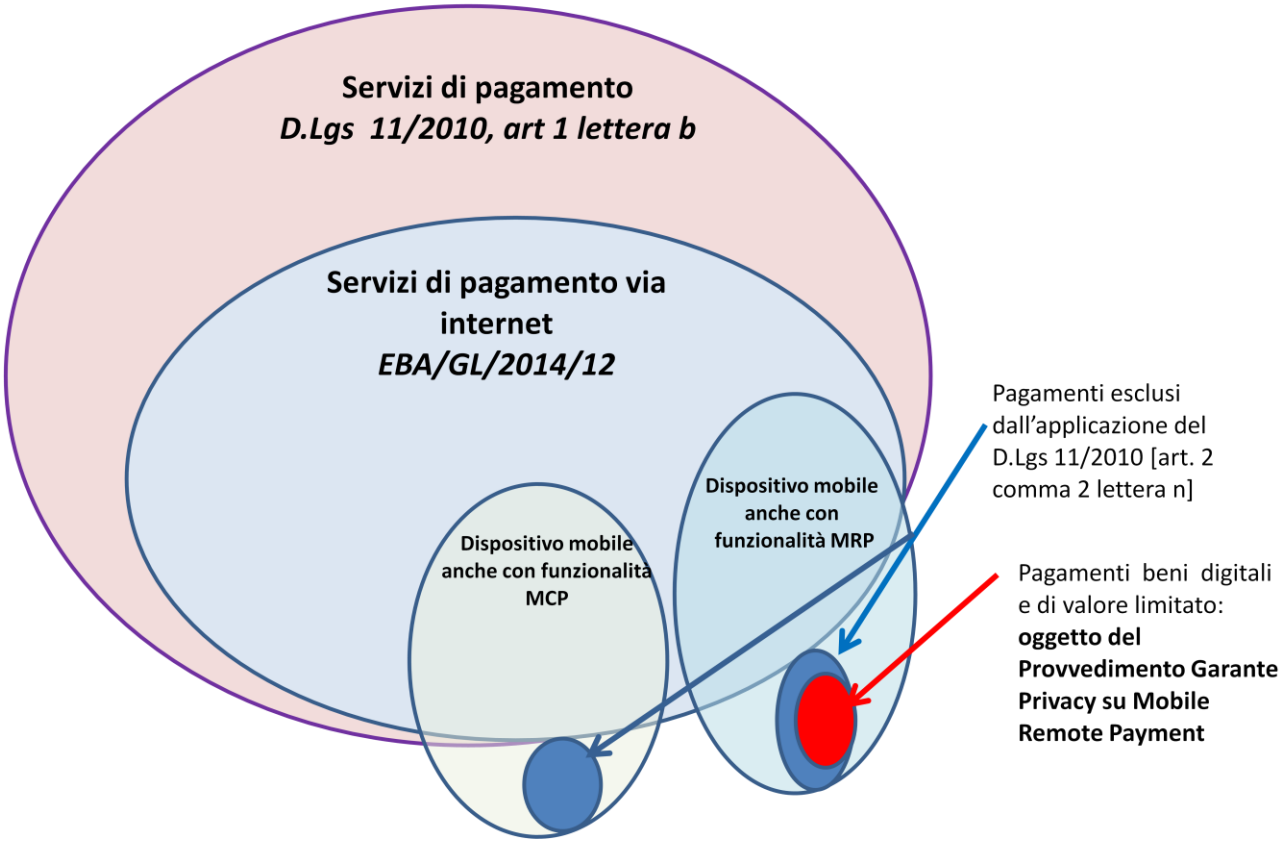
Tabella 2 - Servizi di pagamento inclusi ed esclusi dall'ambito di applicazione della Linea Guida EBA/GL/2014/12

Servizi di pagamento via Internet espressamente inclusi nell'ambito di applicazione della linea guida sulle misure minime di sicurezza per i pagamenti via Internet EBA/GL/2014/12 indipendentmente dal tipo di dispositivo d'accesso utilizzato	Casi espressamente esclusi dall'ambito di applicazione della linea guida EBA/GL/2014/12
• [Carte] esecuzione dei pagamenti con carta su internet, compresi i pagamenti con carte virtuali, così come la registrazione dei dati di carte di pagamento per l'utilizzo in soluzioni "portafoglio"; • [Bonifici] l'esecuzione dei bonifici (Credit Transfers) su Internet; • [E-mandato] l'emissione e la modifica dei mandati elettronici di addebito diretto; • [E-money] trasferimenti di moneta elettronica tra due conti di moneta elettronica via Internet.	- Altri servizi internet forniti da un PSP tramite il suo sito web di pagamento (ad esempio e-intermediazione, contratti on-line); **- I pagamenti in cui l'istruzione è dato per posta, per telefono, posta vocale o utilizzando la tecnologia basata su SMS;** **- Pagamenti mobili diversi dai pagamenti basati su browser;** - CT in cui un terzo accede al conto di pagamento del cliente; - Operazioni di pagamento effettuate da un'impresa tramite reti dedicate;

Le misure di sicurezza richieste dalla Linea Guida EBA/GL/2014/12 devono essere implementate a cura degli enti/aziende PSP (Payment Service Provider ossia i 'Fornitori di servizi di pagamento'). Gli enti/aziende che offrono servizi tecnici (piattaforme tecnologiche, servizi di firma digitale associata ad un pagamento,...) che sono integrati in un servizio di pagamento via Internet, di norma non sono considerati come PSP, per cui comunque la Linea Guida prevede che essi debbano essere contrattualmente tenuti a rispettarla, per la quota parte applicabile al loro servizio tecnico.

La successiva figura illustra invece, nel contesto Italiano, le relazioni di applicabilità della Linea Guida EBA ai servizi di pagamento come definiti nel D.Lgs 11/2010 (ricordiamo: il recepimento della direttiva PSD vigente) ed a quelli per cui è applicabile il Provvedimento del Garante Privacy per il Mobile Remote Control.

Applicabilità delle EBA Guideline e del Provv Garante su Mobile Remote Payment



Le misure minime di sicurezza per i pagamenti effettuati via Internet sono riportate nel documento:

EBA/GL/2014/12: Final guidelines on the security of internet payments

e nella traduzione ufficiale in Italiano predisposta da EBA (cui fa riferimento la nomenclatura qui di seguito utilizzata)

EBA/GL/2014 /12: Orientamenti finali sulla sicurezza dei pagamenti via Internet

3.3 Uno sguardo alla Linea Guida EBA/GL/2014/12

Categoria delle Raccomandazioni presenti nella Linea Guida	*Sottocategorie di Raccomandazioni*
Controllo generale e ambiente di sicurezza (26 specifiche)	Governance
	Valutazione dei rischi
	Monitoraggio e segnalazione degli incidenti
	Controllo e mitigazione dei rischi
	Tracciabilità
Misure specifiche di controllo e di sicurezza per i pagamenti via Internet (30 specifiche)	Identificazione iniziale dei clienti, informazioni
	Autenticazione forte del cliente (Strong customer authentication)
	Iscrizione (enrolment) e fornitura di strumenti e/o software di autenticazione al cliente
	Tentativi di accesso, sessione scaduta, validità di autenticazione
	Monitoraggio delle operazioni
	Protezione dei dati sensibili relativi ai pagamenti
Sensibilizzazione, educazione e comunicazione riguardanti il cliente (11 specifiche)	Educazione e comunicazione riguardanti il cliente
	Comunicazioni, fissazione di limiti
	Accesso dei clienti alle informazioni sullo stato dell'ordine e dell'esecuzione dei pagamenti

Controllo generale e ambiente di sicurezza

Nel loro compesso queste raccomandazioni mappano in modo pressochè completo i corrispondenti controlli previsti dallo standard ISO 27001 relativo alla Gestione della Sicurezza delle Informazioni.

Da notare che nello specifico:

- vi è una forte (come auspicabile attendersi) attenzione all'aspetto del trattamento degli incidenti di sicurezza che prevede la notifica immediata alle autorità competenti (inclusa l'autorità per la protezione dei dati personali) nel caso di gravi incidenti di sicurezza[13]. In particolare i PSP sono invitati a definire contrattualmente con i loro e-merchants[14] gli obblighi, in generale per le misure di sicurezza, e speficamente in caso di incidenti di sicurezza prevedendo, laddove l'e-merchant non risulti cooperare come dovuto nel caso avvenga un simile incidente, penali e/o la rescissione del contratto.
- è previsto un requisto a livello di progettazione dei servizi di pagamento affinchè sia utilizzato il set minimo indispensabile di dati in particolare quelli ritenuti specificamente sensibili (dati delle card,...) nella esecuzione del pagamento: ciò riecheggia i principi di minimizzazione dei dati e non eccedenza rispetto ai fini di trattamento, tipici delle normative in materia di protezione dati personali e utlteriormente rinforzati nella prossima Regolamentazione UE sulla protezione dati personali di prossima emanazione.
- particolare attenzione è rivolta alla tracciabilità delle operazioni connesse alla effettuazione di un pagamento, in termini di meccanismi di sicurezza per la registrazione dettagliata dei dati delle operazioni e dei mandati elettronici, fra cui il numero sequenziale dell'operazione, la marcatura temporale per i dati delle operazioni, le modifiche alla parametrizzazione, e l'accesso ai dati delle operazioni e dei mandati elettronici, con l'obbligo da parte dei PSP di prevedere analisi e verifiche sui relativi log file.

Misure specifiche di controllo e di sicurezza per i pagamenti via Internet

Le raccomandazioni specificate prevedono quanto segue.

> I clienti dei servizi di pagamento via Internet dovrebbero essere adeguatamente identificati in linea con la normativa europea antiriciclaggio e dare conferma della loro volontà di effettuare pagamenti via Internet utilizzando i servizi prima di avere la possibilità di accedere a tali servizi. I PSP dovrebbero fornire ai clienti

[13] cosi definiti nella Linea Guida EBA/GL/2014/12: "*grave incidente per la sicurezza dei pagamenti: un incidente che ha o può avere un impatto significativo sulla sicurezza, sull'integrità e sulla continuità dei sistemi di pagamento dei prestatori di servizi di pagamento e/o sulla sicurezza dei dati sensibili sui pagamenti o dei fondi. La valutazione della rilevanza dovrebbe prendere in considerazione il numero di clienti potenzialmente interessati, l'importo a rischio e l'impatto su altri prestatori di servizi di pagamento o altre infrastrutture di pagamento;*"

[14] ossia coloro che vendono i servizi/beni attraverso i servizi di pagamento via Internet

un’adeguata informazione preventiva e sistematica o, in alcuni casi, 'ad hoc' circa i requisiti necessari (per esempio: apparecchiature, procedure,..) per l’esecuzione in sicurezza di operazioni di pagamento via Internet, nonché i rischi inerenti.

L’inoltro dei pagamenti via Internet, così come l’accesso ai dati sensibili relativi ai pagamenti, dovrebbero essere protetti da un’autenticazione forte (strong authentication) del cliente. I PSP dovrebbero avvalersi di una solida procedura di autenticazione dei clienti.

I PSP dovrebbero garantire che la registrazione iniziale al servizio (enrolment) del cliente e la fornitura iniziale degli strumenti di autenticazione (necessari per utilizzare il servizio di pagamento via Internet) e/o la fornitura di software per effettuare i pagamenti, avvengano in modo sicuro.

I PSP dovrebbero limitare il numero dei tentativi di accesso o di autenticazione, definire le regole per la “scadenza” delle sessioni dei servizi di pagamento via Internet e definire i termini per la validità dell’autenticazione.

I meccanismi per il monitoraggio delle operazioni volti a prevenire, rilevare e bloccare il traffico dei pagamenti fraudolenti dovrebbero essere attivati prima dell’autorizzazione finale del PSP; le operazioni sospette o ad alto rischio dovrebbero essere oggetto di una specifica analisi e procedura di valutazione.

I dati sensibili relativi ai pagamenti dovrebbero essere adeguatamente protetti quando conservati, trattati o trasmessi.

Sensibilizzazione, educazione e comunicazione riguardanti il cliente

Le raccomandazioni specificate prevedono quanto segue.

I PSP dovrebbero fornire assistenza e orientamento ai clienti, ove necessario, per quanto riguarda l’uso sicuro dei servizi di pagamento via Internet. I PSP dovrebbero comunicare con i propri clienti in modo tale da rassicurarli circa l’autenticità dei messaggi ricevuti.

I PSP dovrebbero fissare limiti per i servizi di pagamento via Internet e potrebbero fornire ai loro clienti opzioni per ulteriori limitazioni del rischio entro tali limiti. Essi possono anche fornire servizi di gestione degli avvisi e dei profili dei clienti.

I PSP dovrebbero confermare ai propri clienti l’ordine del pagamento e fornire ai clienti in tempo utile le informazioni necessarie per verificare che l’operazione di pagamento sia stata avviata e/o eseguita correttamente.

3.4 Caso Italia: la consultazione pubblica avviata dalla Banca d'Italia

La Banca d'Italia, in quanto autorità competente a livello nazionale, ha avviato il 12 Agosto 2015 la consultazione pubblica "Recepimento degli Orientamenti dell'ABE sulla sicurezza dei pagamenti via Internet", aperta fino al 12 ottobre 2015, allo scopo appunto di sottoporre a consultazione le modifiche che intende apportare alla disciplina di vigilanza per trasporre nell'ordinamento italiano la Linea Guida EBA/GL/2014/12.

La Banca d'Italia precisa che intende recepire integralmente la Linea Guida EBA/GL/2014/12 per queste categorie di PSP:

- banche
- Poste Italiane SpA, nell'esercizio dell'attività di Bancoposta
- istituti di pagamento
- istituti di moneta elettronica
- intermediari finanziari autorizzati alla prestazione di servizi di pagamento e/o emissione di moneta elettronica

ed evidenzia che la Linea Guida ha lo scopo di innalzare il grado di sicurezza dei pagamenti effettuati tramite il canale internet richiamando espressamente i PSP ad un rispetto puntuale delle misure di sicurezza in essa contenute e delle modalità attuative in essa specificate.

La Banca d'Italia, tenuto conto dell'esito della consultazione, valuterà l'opportunità di concedere un breve termine per l'adeguamento alle disposizioni definitive ed a tal proposito richiederà ai destinatari delle disposizioni definitive di presentare un piano, approvato dall'organo con funzione di supervisione strategica, nel quale dovranno essere individuati e puntualmente definiti gli interventi necessari ad assicurare l'adeguamento al contenuto della Linea Guida, entro un determinato termine per l'attuazione.

3.5 Mapping delle linee guida sicurezza EBA nei controlli CSA

I servizi di pagamento via internet sono il risultato dell'integrazione di un insieme di servizi componenti (gestione borsellino elettronico, servizi di autenticazione acquirenti, servizi di infrastruttura tecnologica, servizi di sicurezza,...) forniti da diversi Provider. Nulla può vietare che tali servizi componenti possano essere di natura cloud based, per cui in tale contesto assume particolare importanza considerare i controlli di sicurezza già individuati dall'organizzaione Cloud Security Alliance con la matrice CSA CCM[15] ed i punti di diretto contatto (mapping) con le misure di sicurezza previste dalla Linea Guida EBA.

Pertanto, in linea con l'attuale impostazione della matrice CSA CCM, che risulta essere già impostata e corredata di più colonne (si tratta di uno foglio elettronico) che riportano il mapping dei controlli CSA rispetto a diverse norme e standard di settore (ad esempio ISO27001, NIST, COBIT) e le più rilevanti leggi privacy americane ed europee, è stata condotta una prima analisi per individuare il mapping anche rispetto alle raccomandazioni presenti nella EBA/GL/2014/12.

Le tabelle successive rappresentano in modo sintetico il risultato dell'attivita' di mapping considerata.

[15] https://cloudsecurityalliance.org/group/cloud-controls-matrix/

Tabella 3 - Sintesi del mapping tra controlli CSA CCM e raccomandazioni EBA/GL/2014/12

Classi di controlli CSA CCM V3.0.1	Numero di controlli CSA CCM mappati in EBA/GL/2014/12	Sottocategorie di raccomandazioni EBA/GL/2014/12 coinvolte nella mappatura nei controlli CSA CCM V3.01
Application & Interface Security	1	- Initial customer identification, information; - Strong Customer authentication; - Enrolment for, and provision of, authentication tools and/or software delivered to the customer
Audit Assurance & Compliance	0	
Business Continuity Management & Operational Resilience	0	
Change Control & Configuration Management	0	
Data Security & Information Lifecycle	1	- Transaction Monitoring
Datacenter Security	1	- Protection of sensitive payment data
Encryption & Key Management	1	- Protection of sensitive payment data
Governance and Risk Management	7	- Governace; - Risk assessment; - Risk control and mitigation
Human Resources	0	
Identity & Access Management	1	- Initial customer identification, information; - Strong Customer authentication; - Enrolment for, and provision of, authentication tools and/or software delivered to the customer
Infrastructure & Virtualization Security	0	
Interoperability & Portability	0	
Mobile Security	0	
Security Incident Management, E-Discovery & Cloud Forensics	1	- Incident monitoring and reporting
Supply Chain Management, Transparency and Accountability	0	
Threat and Vulnerbility Management	0	

Tabella 4 - Elenco delle raccomandazioni EBA/GL/2014/12 non direttamente mappabili nei controlli CSA

Sottocategorie di Raccomandazioni di EBA/GL/2014/12 che non risultano direttamente mappabili nei controlli della CSA CCM V3.0.1:
- Traceability
- Log-in attempts, session time out, validity of authentication
- Customer education and communication
- Notifications, setting of limits
- Customer access to information on the status of payment initiation and execution

Quanto qui realizzato rappresenta solo una prima ipotesi di mapping, che potrà essere successivamente raffinata e rivista concordemente con CSA, responsabile degli aggiornamenti della matrice CSA CCM, in un'ottica di ulteriore completezza individuando anche le correlazioni con i mapping già esistenti tra i controlli CSA CCM verso le normative privacy e verso gli standard di settore 'sicurezza e-payment', già presenti nella attuale matrice, come è il caso dello standard PCI DSS[16].

4.0 Nota sulle valute virtuali: fattori di successo e fattori di rischio

4.1 Introduzione sulle Valute Virtuali

Le c.d. valute virtuali (VV) sono rappresentazioni digitali di valore non emesse da una banca centrale o da un'autorità pubblica. Esse non sono necessariamente collegate a una valuta avente corso legale, ma sono utilizzate come mezzo di scambio o detenute a scopo di investimento e possono essere trasferite, archiviate e negoziate elettronicamente. È molto importante sottolineare come le VV non possano considerarsi moneta legale nè devono essere confuse con la moneta elettronica. Negli ultimi anni si è assistito ad una crescente diffusione delle VV nel panorama internazionale.

Attualmente, sono oltre 500 i modelli esistenti nel mondo, il più famoso dei quali è **bitcoin**. Il fenomeno è stato oggetto di considerazione da parte di numerose autorità internazionali, governi, banche centrali e autorità di vigilanza, interessati a comprendere se, ed eventualmente in che modo, regolamentarlo. A luglio 2014, l'Autorità Bancaria Europea (European Banking Authority, EBA) ha pubblicato un parere sulle VV[17], al fine di favorire un processo di convergenza regolamentare a livello europeo. In particolare, l'EBA ha individuato numerosi profili di rischio derivanti dall'utilizzo o dalla detenzione delle VV. Essi sono rilevanti per gli utilizzatori (consumatori, investitori e merchant), per i partecipanti al mercato - piattaforme di scambio e depositari dei portafogli virtuali (wallet providers) - per gli intermediari e le autorità di regolamentazione, oltre che per l'integrità e la stabilità del sistema finanziario e del sistema dei pagamenti.

Certamente, nel corso dell'ultimo decennio, in funzione dell'evoluzione di Internet, i tentativi di realizzare una moneta cibernetica (cybercoin) o denaro digitale, sono stati molteplici e legati soprattutto al crescente sfruttamento della Rete per il commercio elettronico (E-commerce). Il commercio online, a livello mondiale, è in crescente espansione e solo in Italia, secondo un recente studio condotto dall'osservatorio Netcomm-Polimi, si

[16] Il PCI Security Standards Council propone e gestisce standard per migliorare la sicurezza dei dati principalmente nell'utilizzo delle carte di pagamento (https://it.pcisecuritystandards.org/security_standards/)
[17] Rinvenibile al seguente URL: http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

attesta a un +18% con un giro di affari stimato per il 2012 pari a 9,5 miliardi di euro[18]. Naturalmente il sistema di pagamento elettronico rappresenta la "spina dorsale" su cui si basa l'E-commerce, che si traduce in un pagamento virtuale che sostituisce il passaggio fisico di denaro. Solitamente i sistemi di E-Cash sono gestiti da società private, che non necessariamente corrispondono a istituti di credito o società finanziarie. Sono prevalentemente aziende che operano nel settore dell'E-commerce, che sviluppano sistemi web-based mediante i quali è possibile ottenere denaro elettronico previo versamento su un conto corrente bancario di una somma di denaro fisico. Con il denaro elettronico è possibile eseguire qualsiasi operazione finanziaria con tutte le organizzazioni operanti in Internet o che sono convenzionate con i gestori di un particolare sistema di moneta elettronica. Naturalmente, per ogni operazione di esborso di denaro elettronico (riconducibile ad un acquisto di un bene/servizio), ne corrisponde una equivalente di prelevamento sul deposito che custodisce il denaro reale. La società che ha in deposito il denaro dell'utente si occuperà del trasferimento della somma alla struttura in cui l'utente ha compiuto l'acquisto. In sostanza si tratta di carte di pagamento che possono consentire di portare a termine transazioni finanziarie sicure, grazie all'implementazione di apposite procedure di autenticazione[19] .

Le valute virtuali vanno quindi a inserirsi fra la figura della carta di credito o di debito e la moneta reale. La differenza sostanziale tra le carte di credito e i sistemi che si basano su moneta virtuale, è rappresentata principalmente dalla regolamentazione legislativa. Mentre le prime sono emesse e gestite da istituti di credito e società finanziarie, quindi sottoposte a norme e regolamenti vigenti nelle rispettive nazioni e da accordi internazionali che ne regolamentano le operazioni, nel caso del denaro elettronico si tratta di operazioni gestite da società che operano nel web, non riconducibili ad organismi istituzionali e quasi mai a banche internazionali e operanti in contesti transnazionali. In tal senso l'extraterritorialità può costituire un serio problema per la validità delle operazioni, ma, soprattutto, per la possibile mancanza di trasparenza nelle transazioni finanziarie effettuate.
Anche se comode nel loro utilizzo e certamente più sicure nelle fasi di erogazione del denaro, le carte di pagamento sono rimaste confinate nel web per utilizzi per lo più finalizzati ad acquisti online. Ma da qualche anno, un nuovo tentativo di introduzione sul mercato virtuale di una nuova moneta elettronica, sembra aver preso la direzione giusta e la repentina scalata del suo utilizzo, sembra confermarne il successo.
Si chiama Bitcoin (moneta digitale) e le sue maggiori peculiarità risiedono nell'anonimato e nella non rintracciabilità.

[18] Fonte: http://gnosis.aisi.gov.it/Gnosis/Rivista31.nsf/ServNavig/11

[19] Si tratta di procedure che sono realizzate da società che gestiscono denaro elettronico e consistono nell' utilizzo di sistemi tecnologici (hardware e software) per garantire all' utente che il suo denaro non venga prelevato da malintenzionati per effettuare acquisti a suo nome. Solitamente, l' utente che attiva un conto di deposito, deve scaricare sul proprio personal computer un programma appositamente creato dalla società che gestirà il conto. Successivamente, dovrà utilizzare l' applicativo ogni volta che vorrà effettuare acquisti in rete. Generalmente, questi software prevedono, oltre a delle credenziali di identificazione (username e password), anche dei codici di criptazione.

4.2 Il Bitcoin, la VV di maggior successo

Nata da pochi anni, la VV Bitcoin si caratterizza come un protocollo di comunicazione prevalentemente utilizzato come veicolo di valuta virtuale il cui successo è pressocchè assoluto nonchè caratterizzato da numerose peculiarità. Gli utenti (client) fruiscono in modo paritario delle stesse risorse, condividendo gli stessi dati a velocità maggiori rispetto quelle di un sistema di tipo client-server, in cui il computer che offre i suoi servizi (server) essendo costretto a soddisfare le richieste di più client, rischia di rallentare, anche in maniera rilevante, la velocità di trasmissione dei dati. Inoltre, in termini di sistema P2P la sicurezza degli accessi ai client viene gestita localmente, su ogni singola macchina, fattore che presuppone una standardizzazione degli archivi per ogni nodo.

Il database che contiene le informazioni è distribuito tra i nodi della rete e si occupa anche della conferma delle transazioni e di impedire che si possano spendere due volte le stesse monete. Le operazioni sono tutte tracciate e i trasferimenti di Bitcoin, tra conti pubblici dei nodi, sono cifrate grazie all'utilizzo del sistema di crittografia a chiave pubblica[20], che garantisce un discreto grado di sicurezza e protezione ai dati trasmessi. Lo scopo di Bitcoin è essenzialmente quello di consentire il possesso e il trasferimento anonimo del denaro digitale. Altra peculiarità di questa VV è che possono essere spesi solo dal legittimo proprietario, che può farlo una sola volta per lo stesso denaro impedendo, quindi, che si possa spendere la stessa moneta digitale per più volte. Il controllo sulle somme spese, è garantito dal database distribuito, che memorizza tutte le transazioni che vengono effettuate, pubblicizzandole a tutti i nodi.

Ogni fruitore della rete Bitcoin possiede un portafoglio che contiene un numero arbitrario di coppie di chiavi asimmetriche. Le chiavi pubbliche, identificabili anche come indirizzi Bitcoin, costituiscono gli identificativi dei nodi di trasmissione e/o ricezione per tutte le transizioni di cybercoin. Altra caratteristica importante risiede nel fatto che gli indirizzi Bitcoin non contengono alcuna informazione che possa ricondurre al legittimo proprietario, funzione che ne garantisce l'anonimato.

Per quanto concerne le modalità di utilizzo del sistema, chiunque può dotarsi del software apposito, senza alcun costo e scaricandolo direttamente dalla rete. Dopo aver effettuato il download e l'installazione automatica e guidata del programma, esso procede autonomamente ad aggiornare tutte le transazioni effettuate sui diversi nodi della rete. L'applicativo provvede anche alla generazione di un indirizzo bitcoin, in forma leggibile, con sequenze casuali di numeri e cifre lunghe in media 33 caratteri, che cominciano sempre per 1, della forma tipo: 1Ai83aafRLWYtMDNbP8b3uiWyquun6ot46.

È importante porre l'accento sulla possibilità concessa all'utente di ottenere un numero infinito di indirizzi Bitcoin, dato che la generazione delle coppie di chiavi non interferisce in alcun modo con gli altri nodi della rete.

---

[20] Crittografia. La crittografia è quel settore scientifico che si occupa dei sistemi e delle tecniche per rendere un messaggio " nascosto" o non comprensibile a persone non autorizzate a leggerlo. Lo studio della crittografia e della crittoanalisi si chiama comunemente crittologia. La crittografia a chiave pubblica o crittografia asimmetrica, si basa sull' utilizzo di una coppia di chiavi: la chiave pubblica deve essere distribuita in rete e serve a cifrare un documento destinato alla persona che possiede la relativa chiave privata; la chiave privata, personale e segreta, viene utilizzata per decifrare un documento cifrato con la chiave pubblica.

Il vantaggio del possesso di più coppie di chiavi, risiede nella maggiore garanzia di anonimato, grazie alla possibilità di utilizzare una coppia di chiavi diversa per ogni transazione effettuata. Il funzionamento della chiave asimmetrica è relativamente semplice. L'indirizzo Bitcoin contiene la chiave pubblica del suo destinatario, che viene consegnata all'atto della transazione monetaria[21]. La transazione viaggia attraverso i nodi, che provvedono alla validazione delle firme crittografiche e all'ammontare della somma oggetto della transazione.

L'aspetto più peculiare del sistema è rappresentato dal sistema di controllo delle somme impegnate per impedire che le stesse somme siano utilizzate per più transazioni (sistema di marcatura oraria peer-to-peer). In sostanza, per ogni transazione viene assegnato un identificatore sequenziale, che ne impedisce la manomissione in funzione di un sistema di conferme a catena. Le conferme sono attribuite dai diversi nodi coinvolti mediante una lista di marcatura oraria che è gestita collettivamente dagli stessi nodi (catena dei blocchi). Il funzionamento della catena a blocchi, si basa su di una serie di controlli e verifiche che implementano algoritmi matematici che mirano a trasformare una transazione da "non confermata" a "confermata". È importante rilevare che la catena di blocchi conserva tutto lo storico delle transazioni effettuate, con tutte le indicazioni riconducibili agli indirizzi Bitcoin e all'ammontare delle somme erogate e ricevute. Pertanto, se un utente prova a riutilizzare Bitcoin che ha già speso, la rete peer-to-peer rifiuterà la transazione perché non risulterà più essere lui proprietario della somma. I Bitcoin possono essere trasferiti attraverso la rete a chiunque disponga di un indirizzo Bitcoin.

Al momento dell'installazione del programma viene scaricato il database completo delle transazioni, che al momento è ancora piuttosto contenuto (nei primi giorni di maggio 2012 raggiungeva la soglia di circa 200.000 transazioni), per fare in modo che tutti gli utenti possano avere a disposizione l'intero archivio. Tuttavia, nel caso in cui il database dovesse assumere dimensioni considerevoli, è previsto che gli utenti possano scaricare solo una parte di esso, eliminando le transazioni datate o di scarso interesse personale.

Quindi, la rete Bitcoin crea e distribuisce monete virtuali automaticamente sui nodi della rete che mantengono abilitata, sul proprio computer, l'opzione del programma "genera Bitcoin". Questa moneta viene distribuita in "blocchi" che non superano mai l'ammontare di 50 BTC. Generalmente viene richiesta una piccola "tassa di transazione" per ogni operazione condotta, che viene suddivisa tra i nodi che partecipano alla gestione del traffico generato. Dato che i nodi non sono costretti ad includere le transazioni nei blocchi che si generano, chi invia Bitcoin è stimolato a pagare la tassa per agevolare e velocizzare le proprie transazioni sui diversi nodi del sistema. In questo modo si stimolano i proprietari dei nodi a tenerli costantemente "attivi".

Al momento attuale, il rapporto Bitcoin/€ è il seguente:

[21] Facendo un esempio, supponiamo che il Sig. Rossi intenda trasferire una somma di Bitcoin al Sig. Verdi. Rossi inserirà la chiave pubblica di Verdi nell'effettuare l'operazione, contrassegnando la trasmissione del denaro con la sua chiave privata (segreta e nota soltanto a Rossi).

BTC/EUR Panoramica

Precedente	202,92	Denaro	204,10	Min-Max gg	200,89 - 205,57
Apertura	202,92	Lettera	205,00	52 settimane	144.10 - 3200.00
Rendiconto 1 anno	-45,31%				

[22]

Nonostante i Bitcoin siano apparsi sul mercato relativamente da pochi anni, il successo è stato rapido e capillare, attivando un mercato variegato che spazia dagli acquisti nel settore immobiliare a quello delle automobili usate. Numerosi siti offrono la possibilità di cambiare Bitcoin con diverse valute, come Dollari statunitensi, Euro, Rubli e Yen. Parte del successo è riconducibile al fatto che, contrariamente a ciò che accade per le monte a corso legale, i Bitcoin non sono controllati da nessun organismo che ne possa modificare l'effettivo valore. La decentralizzazione del Bitcoin ne rappresenta un indiscusso valore aggiunto, in funzione del fatto che non risente delle possibili instabilità economico-finanziarie che possono essere ricondotte ai comportamenti delle banche centrali (cosa che accade quasi sistematicamente per le altre monete a corso legale). Pertanto il rischio di inflazione della moneta risulta di fatto irrealizzabile, ananche perchè la quantità di Bitcoin è stata limitata ad un importo prestabilito. Quest'ultima caratteristica potrebbe contribuire, nel tempo, all'attivazione del processo di deflazione della moneta, che consiste nell'incremento del valore reale della stessa.
Gli unici due aspetti che sarebbero in grado di influenzare negativamente lo sviluppo dell'utilizzo dei Bitcoin, sono la diminuzione degli utilizzatori della moneta elettronica e un possibile attacco dei governi alla fruizione della stessa.

[22] http://it.investing.com/currencies/btc-eur

4.3 I fattori di rischio connaturati alle Valute Virtuali: profili penali

I fattori di rischio presenti nel concetto stesso delle VV derivano necessariamente dalla loro difficile tracciabilità e sostanziale aleatorietà della trasmissione. Alcuni di tali rischi si sono già concretizzati in gravi perdite o furti di VV per la clientela, nel fallimento di piattaforme di scambio o in attività di riciclaggio e altre condotte criminali[23]. Secondo l'Autorità Bancaria Europea, i rischi individuati superano i possibili benefici che le VV potrebbero fornire ai loro utilizzatori, anche considerando i vantaggi in termini di costi e tempi di transazione e di inclusione finanziaria. Auspicando un intervento delle istituzioni europee, l'EBA ha evidenziato la necessità di definire, nel lungo periodo, un quadro normativo armonizzato, che riservi l'operatività in VV a soggetti autorizzati e definisca, tra l'altro, requisiti in materia di capitale e governance dei partecipanti al mercato e segregazione dei conti della clientela. Nel breve termine, ha ravvisato l'urgenza di mitigare i rischi derivanti dall'interazione tra gli schemi di VV e i servizi finanziari regolamentati ed ha, pertanto, invitato le Autorità nazionali di vigilanza a scoraggiare gli intermediari dall'acquistare, detenere o vendere VV. In tale contesto, gli intermediari potrebbero invece continuare a offrire a soggetti operanti nel settore delle VV, le attività e i servizi finanziari alla cui prestazione sono autorizzati. Dal punto di vista della regolamentazione italiana, recentemente è stato prodotto il documento "Avvertenza sull'uso delle cd. valute virtuali", pubblicato sul sito internet della Banca d'Italia[24].

La Banca d'Italia condivide, infatti, l'opinione dell'EBA di scoraggiare le banche e gli altri intermediari vigilati dall'acquistare, detenere o vendere VV. Gli intermediari vigilati dalla Banca d'Italia vanno quindi esortati a valutare con attenzione i rischi indicati dall'EBA ed a considerare che:

- in assenza di adeguati presidi e di un quadro legale certo circa la natura giuridica delle VV, quei rischi possono esporre a perdite e inficiare, di conseguenza, la consistenza del patrimonio di vigilanza e la stabilità stessa degli intermediari;
- le concrete modalità di funzionamento degli schemi di VV possono integrare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati (artt. 130, 131 TUB per l'attività bancaria e l'attività di raccolta del risparmio), senza dimenticare la macroarea del riciclaggio di denaro sporco da parte di attività criminali organizzate.

Da un punto di vista di allarme sociale, il riciclaggio è il reato decisamente più rilevante fra quelli che interessano il mondo delle valute virtuali. L'art. 648-bis del Codice Penale prevede quanto segue:

[23] È il caso del fallimento della nota piattaforma di scambio giapponese Mt. Gox, avvenuto nei primi mesi del 2014, a seguito di un attacco informatico, che ha comportato la perdita di circa 750 mila Bitcoins di proprietà di migliaia di utenti. Si segnala inoltre il caso della piattaforma di scambio Bitcoinica, più risalente nel tempo (2012), anch'essa oggetto di un attacco informatico, con conseguenti perdite di Bitcoins a carico degli utenti.

[24] http://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf

- "[1] *Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000. [2] La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. [3] La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648."*

Il riciclaggio è un delitto che prevede la reclusione dai 4 ai 12 anni nonché la multa fra i 5000 ed i 25000 euro. La condotta è riconducibile in ogni attività di sostituzione, trasferimento o compimento di altre operazioni di denaro, beni o altre utilità provenienti da un delitto doloso, così da ostacolarne l'identificazione delittuosa. Spesso accade che i reati base si configurino nei delitti di associazione a delinquere o associazione mafiosa, le quali "puliscono" il denaro o i beni di origine criminosa impiegandoli in attività tali da ricavarne denaro pulito. All'interno del mondo delle VV, ben chiari appaiono i rischi che si celano dietro questo tipo di monete, fintanto che risulterebbe molto facile sfruttarle al fine di riconvertire, ad esempio, in bitcoins, del denaro di origine delittuosa per poi acquistare con la VV ulteriori beni e utilità di modo da eliminare la traccia sporca del denaro a monte.

Per quanto concerne i reati previsti nel TUB(Testo unico Bancario)[25], l'art. 130, rubricato (Abusiva attività di raccolta del risparmio), prevede che:

- Chiunque svolge l'attività di raccolta del risparmio tra il pubblico in violazione dell'articolo 11 è punito con l'arresto da sei mesi a tre anni e con l'ammenda da euro 12.911 a euro 51.645.

Trattasi, in questo caso, di una contravvenzione non oblabile (il che significa che non può essere "scontata" col semplice pagamento dell'ammenda, ma prevede necessariamente sia l'arresto che l'ammenda) che punisce chiunque svolge l'attività di raccolta di risparmio senza rispettare quanto previsto dall'art. 11. Quest'articolo prevede che ai fini del TUB sia considerata raccolta del risparmio l'acquisizione di fondi con obbligo di rimborso, sia sotto forma di depositi sia sotto altra forma, vietando la raccolta al pubblico a soggetti diversi dalle banche. Al comma 2-bis, prevede che non costituisce raccolta del risparmio tra il pubblico la ricezione di fondi connessa all'emissione di moneta elettronica. Dunque la legge, tramite questo innesto, ha vietato lo sfruttamento della moneta elettronica con la finalità di svolgere un attività di risparmio fra il pubblico.

Venendo al più grave articolo 131, è qui punita la condotta di chi, oltre a svolgere attività di raccolta del risparmio di cui sopra in violazione dell'art. 11, vada poi ad esercitare il credito. In questo caso trattasi non più di contravvenzione bensì di delitto punito da 6 mesi a 4 anni e con la multa da euro 2.065 fino a euro 10.329. In questo reato è quindi represso l'esercizio abusivo di attività bancaria. L'esercizio del credito è senza dubbio l'attività di intermediazione finanziaria più comune e diffusa; integrano infatti esercizio del credito i finanziamenti sotto qualsiasi forma, la locazione finanziaria, l'acquisto di crediti e le altre operazioni che il d.m. 6 luglio 1994 classifica allo stesso modo. Esulano, invece, da tale nozione le attività riservate agli intermediari iscritti nell'elenco previsto dall'art. 106: intermediazione dei cambi, attività di prestazione e gestione di servizi di

[25] Decreto legislativo 1° settembre 1993, n. 385 Testo unico delle leggi in materia bancaria e creditizia Versione aggiornata al decreto legislativo 12 maggio 2015, n. 72
http://www.bancaditalia.it/compiti/vigilanza/intermediari/TUB_giugno_2015.pdf

pagamento, assunzioni in partecipazione e le altre operazioni "attive" contemplate dall'art. 7 del d.m. 6 luglio 1994.

Interessante infine la figura dell'art. 131-ter che prevede che:

- Chiunque presta servizi di pagamento in violazione della riserva prevista dall'articolo 114-sexies senza essere autorizzato ai sensi dell'articolo 114-novies è punito con la reclusione da sei mesi a quattro anni e con la multa da 2.066 euro a 10.329 euro.

Il richiamo all'art. 114-bis introduce nella condotta criminosa la figura dell'emissione di moneta elettronica. Tuttavia, non bisogna cadere nell'errore di ritenere la VV o i Bitcoin delle monete elettroniche, in quanto queste non sono espressamente regolamentate. Infatti La moneta elettronica è "*un valore monetario rappresentato da un credito nei confronti dell'emittente che sia memorizzato su un dispositivo elettronico, emesso previa ricezione di fondi di valore non inferiore al valore monetario emesso e accettato come mezzo di pagamento da soggetti diversi dall'emittente*" (art. 55, lett. h ter della Legge n. 39 del 1 marzo 2002, attuativa della Direttiva 2000/46/CE). Rientreranno dunque in questo concetto, ad esempio, le carte di pagamento prepagate e i conti di tipo prepagati.

In conclusione, dunque, una moneta decentralizzata e virtuale quale il Bitcoin, senza alcun "valore" sottostante a garanzia e con una totale assenza di regolamentazione, espone l'utilizzatore ad ulteriori rischi rilevanti, tra cui:

- Possibilità di fallimento: ciò potrebbe avvenire per svalutazione della moneta, attacchi speculativi, diminuzione degli utenti, introduzione di regolamentazione da parte di Governi, introduzione di criptovalute più efficienti. Non è però possibile bandire ogni forma di denaro digitale quali i bitcoin. In caso di default, non essendo garantito il bitcoin da alcun Governo né avendo alcun rapporto sottostante, i possessori di bitcoin non avrebbero alcun indennizzo.
- Rischi di Frode informatica: Essendo la transazione irreversibile su internet, la vulnerabilità informatica può comportare la compromissione degli account.
- Anonimato: tale aspetto potrebbe compromettere l'intero sistema per il rispetto proprio delle normative antiriciclaggio (alcune banche non accettano conti di società che compiono transazioni in bitcoin). Nelle criptovalute più che di sistema anonimo è preferibile parlare di sistema pseudonimo, per la possibilità di creare innumerevoli account per trasferire i bitcoin, con difficoltà di rintracciabilità delle controparti.
- Utilizzo per fini illeciti: la decentralizzazione e l'assenza di organi di controllo possono esporre la criptovaluta a utilizzo per fini criminali, com'è avvenuto negli USA[26].

[26] Il Federal Bureau of Investigation (FBI) ha chiuso e sequestrato il sito SilkRoad che utilizzava bitcoin per traffici illegali sequestrando criptovaluta. (http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announcesseizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbrichtalleged-owner-and-operator-of-silk-road-website), arrestandone il gestore (http://www.fbi.gov/newyork/press-releases/2014/manhattan-u.s.-attorney-announcesthe-indictment-of-ross-ulbricht-the-creator-and-owner-of-the-silk-road-website). Un altro caso è l'arresto del CEO di Bitinstant.com Charlie Shrem per violazione delle normative antireciclaggio.

5.0 Acronimi

EBA	European Banking Authority
EDPS	European Data Protection Supervisor
EDPS	European Data Protection Supervisor
EMD	Electronic Money Directive (attualmente identifica la direttiva europea 2009/110/CE)
EPC	European Payment Council
IMEL	Istituti Emittenti di Moneta elettronica (IMEL)
MCP	Mobile Contactless Payment
MRP	Mobile Remote Payment
PSD	Payment Service Directive (attualmente identifica la direttiva europea 2007/64/CE
PSP	Payment Service Provider ossia i Fornitori di Servizi di Pagamento
SecuRe Pay	European Forum on the Security of Retail Payments
SMS	Short Message Service
TUB	Testo Unico Bancario
VV	Valuta Virtuale

6.0 Bibliografia

[1]	Decreto Legislativo 196/03 30 Giugno 2003 e s.m.i.
[2]	Allegato B "Disciplinare tecnico in materia di misure minime di sicrezza" del D.Lgs 196/03
[3]	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 *(G.U. n. 300 del 24 dicembre 2008)*
[4]	Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) - 4 aprile 2013 e REGOLAMENTO (UE) N. 611/2013 DELLA COMMISSIONE del 24 giugno 2013 sulle misure applicabili alla notifica delle violazioni di dati personali a norma della direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche
[5]	Recepimento normativo in tema di dati di traffico telefonico e telematico (provvedimento del Garante Privacy del 17-01-2008 come aggiornato al 24-07-2008)
[6]	Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014 *(Pubblicato sulla Gazzetta Ufficiale n. 280 del 2 dicembre 2014)*
[7]	EBA/GL/2014/12 Appendix 1 21 May 2015 Updated 31 July 2015 EBA/GL/2014/12: Appendix 1 Compliance Table - Guidelines Based on information supplied by them, the following competent authorities comply or intend to comply with: EBA Guidelines EBA/GL/2014/12 on the security of internet payments, published on 19th December 2014.