assonime

Associazione fra le società italiane per azioni

13/2013

Note e Studi

Identificazione on-line e pagamenti elettronici: semplicità, sicurezza e interoperabilità

Questo rapporto è stato elaborato dal gruppo di lavoro su "Digitalizzazione e attività d'impresa: la prospettiva europea", istituito nell'ambito della Giunta di Assonime.
Il gruppo di lavoro è coordinato da Pietro Guindani. I componenti del gruppo sono: Patrizia Albano, Cesare Avenia, Franco Bassanini, Pietro Boroli, Salvatore Cardillo, Elio Catania, Andrea Colaneri, Paolo D'Amico, Paolo Di Domenico, Alberto Fabbri, Claudio Giua, Piergaetano Marchetti, Eduardo Montefusco, Claudio Ongaro, Roberto Parazzini, Maurizio Poerio, Luca Sanfilippo, Alessandra Santacroce, Fabrizio Savi, Maurizio Sella, Marco Zuppi.
Il rapporto segue i policy paper già pubblicati dal Gruppo di lavoro sui temi della tutela dei dati personali e della protezione dei diritti di proprietà intellettuale nel contesto on-line.
Alla stesura hanno collaborato Ginevra Bruzzone e Annalisa Oresta di Assonime.

Indice

Executive summary

Introduzione p. 6

1. Identificazione elettronica e firme elettroniche p. 9

1.1 Caratteristiche dei processi di identificazione elettronica ed esigenze degli utenti p. 9

1.2 Il quadro normativo europeo vigente p. 12

1.3 La proposta di regolamento sull'identificazione elettronica e i servizi fiduciari p.15

1.4 L'impatto della nuova disciplina europea: quali sfide per l'Italia p.22

2. I pagamenti elettronici nell'Agenda digitale p.27

2.1 La diffusione dei pagamenti elettronici p.27

2.2 Le iniziative europee p.30

2.3 Le iniziative in Italia p.34

Executive Summary

L'economia digitale può contribuire in maniera significativa all'innalzamento della crescita economica. Oggi circa 2,5 miliardi di individui, il 35 per cento della popolazione mondiale, utilizzano internet; le linee di telefonia cellulare sono quasi 6 miliardi. Per sfruttare appieno le opportunità offerte dalla digitalizzazione occorre mettere a disposizione dei cittadini e delle imprese strumenti di identificazione e pagamento di semplice utilizzo, con caratteristiche di sicurezza adeguate alle diverse esigenze e interoperabili. Ciò richiede processi di standardizzazione e un quadro normativo adeguato, preferibilmente da sviluppare a livello europeo.

Identificazione elettronica

La normativa europea sinora si è concentrata sulle firme elettroniche ed è stata applicata in modo difforme negli Stati membri. Il Parlamento europeo e il Consiglio stanno discutendo un progetto di regolamento sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno, volto a migliorare il mutuo riconoscimento e l'utilizzo transfrontaliero di vari strumenti utili per la realizzazione delle transazioni on-line: identificazione elettronica, firme elettroniche, sigilli elettronici per le persone giuridiche, validazione temporale elettronica, documenti elettronici, servizi elettronici di recapito. Questo progetto merita pieno sostegno; al tempo stesso, occorre indirizzare da subito le scelte di *policy* nazionali in direzioni conformi al futuro diritto europeo.

Nel nostro ordinamento già alla fine degli anni Novanta furono introdotte disposizioni sul valore giuridico del documento informatico. Negli anni recenti vi è stato un forte impulso alla diffusione della firma digitale, prevedendone l'utilizzo obbligatorio per imprese e professionisti nei rapporti con il settore pubblico. La diffusione delle altre tipologie di firma (firme avanzate e in particolare firme qualificate diverse dalla firma digitale) è stata invece rallentata dal ritardo nell'adozione delle regole tecniche previste dal Codice dell'amministrazione digitale, adottate solo nel febbraio 2013. Si dovrebbe ora procedere a emanare rapidamente le restanti regole tecniche (sul documento informatico, la conservazione, la gestione dei flussi documentali e il protocollo informatico).

La frammentazione della *governance* dell'Agenda digitale ha frenato i provvedimenti attuativi: il recente rafforzamento delle competenze della Presidenza del Consiglio dei ministri dovrebbe assicurare un'azione più incisiva.

Tra le iniziative da considerare strategiche a livello italiano vi sono la realizzazione di un sistema integrato per la gestione dell'identità digitale dei cittadini e delle imprese, volto a

semplificare e rendere più sicura l'interazione con la pubblica amministrazione, e la realizzazione dell'Anagrafe nazionale della popolazione residente.

Pagamenti elettronici

La diffusione dei pagamenti elettronici costituisce un importante obiettivo per la politica pubblica: essa può ridurre significativamente i costi di gestione per gli operatori e semplificare l'acquisto dei beni e servizi da parte dei consumatori.

La Commissione europea ha recentemente presentato una proposta di direttiva sui servizi di pagamento nel mercato interno, volta a sostituire la direttiva 2007/64/CE. L'obiettivo, condivisibile, è contemperare l'esigenza di favorire lo sviluppo di nuovi servizi con quella di garantire la sicurezza e la tutela dei dati personali, creando una parità di condizioni concorrenziali, senza distorsioni. Spetta invece alla standardizzazione il compito di assicurare l'interoperabilità delle soluzioni nel settore dei pagamenti, anche in relazione allo sviluppo dei nuovi servizi.

In Italia nell'ultimo biennio sono state adottate varie disposizioni volte a favorire la diffusione dei pagamenti elettronici. Ne è derivato, tra l'altro, un rapido sviluppo del mercato dei pagamenti del trasporto pubblico locale con dispositivo mobile. Numerose disposizioni mirano a incentivare il ricorso ai pagamenti elettronici prevedendone l'utilizzo nei rapporti con la pubblica amministrazione. Nella maggior parte dei casi, l'efficacia delle disposizioni dipende dall'adozione di misure attuative. Il completamento della disciplina dovrebbe essere visto come una priorità dell'Agenda digitale italiana.

Introduzione

I nuovi servizi resi disponibili dall'economia digitale hanno profondamente mutato i comportamenti delle persone, modificando il modo di comunicare, di lavorare, di informarsi. Oggi circa 2,5 miliardi di individui, il 35 per cento della popolazione mondiale, utilizzano internet; le linee di telefonia cellulare sono quasi 6 miliardi. Le nuove tecnologie hanno inoltre trasformato il modo di operare delle imprese, favorendo l'innovazione di processo, la penetrazione di nuovi mercati, la realizzazione di nuovi prodotti e servizi, l'adozione di più efficienti assetti organizzativi. Nel settore dei servizi finanziari, per esempio, oltre il 50 per cento delle piccole e medie imprese europee, pur in presenza di forti differenziazioni geografiche, utilizza sistemi di *home/Internet banking*.

Creare condizioni favorevoli allo sviluppo dell'economia digitale è una delle linee direttrici fondamentali per la promozione della crescita economica e dello sviluppo sostenibile, consentendo di ottimizzare le risorse disponibili, rilanciare la produttività delle imprese e del lavoro, sviluppare nuove opportunità, migliorare la vita quotidiana dei cittadini.

L'Agenda digitale europea, adottata dalla Commissione europea nel 2010 come una delle componenti della più ampia strategia Europa 2020, individua una serie di misure volte a creare un ambiente funzionale allo sviluppo delle transazioni on-line e alla realizzazione del mercato unico digitale in Europa[1]. Il piano d'azione, delineato attraverso successivi documenti[2], ha l'obiettivo di raddoppiare entro il 2015 la quota del commercio elettronico sulle vendite al dettaglio (pari al 3,4 per cento nel 2010) e la quota del settore internet sul Pil europeo (inferiore al 3 per cento nel 2010). Secondo le stime della Commissione europea, la piena attuazione del programma consentirebbe di aumentare il Pil europeo del 5 per cento nei prossimi otto anni e di creare circa 4 milioni di nuovi posti di lavoro distribuiti in tutti i settori dell'economia.

Per conseguire l'obiettivo, occorre agire su più fronti.

Le cinque priorità dell'azione europea per lo sviluppo del commercio elettronico sono:

- sviluppare regole giuridiche che facilitino l'offerta transfrontaliera on-line di prodotti e servizi;

[1] Comunicazione della Commissione, *Un'agenda digitale europea*, COM(2010) 245 def., 26 agosto 2010.

[2] Comunicazione della Commissione, *L'Atto per il mercato unico. Dodici leve per stimolare la crescita e rafforzare la fiducia – Insieme per una nuova crescita*, COM(2011) 206 def., 13 aprile 2011; comunicazione della Commissione, *Un quadro coerente per rafforzare la fiducia nel mercato unico digitale del commercio elettronico e dei servizi* on-line, COM(2011) 942 def., 11 gennaio 2012; comunicazione della Commissione, *L'Atto per il mercato unico II - Insieme per una nuova crescita*, COM(2012) 573 def., 3 ottobre 2012. Cfr. Anche il Commission Staff Working Document, *Report on the implementation of the e-commerce action plan*, pubblicato il 23 aprile 2013.

- migliorare l'informazione degli operatori e rafforzare la protezione dei consumatori;
- assicurare sistemi affidabili ed efficienti di pagamento e di consegna dei prodotti;
- contrastare i comportamenti fraudolenti e sviluppare sistemi efficaci di risoluzione delle controversie;
- realizzare le reti a banda larga e promuovere soluzioni tecnologiche avanzate[3].

Gli interventi ritenuti oggi più urgenti per realizzare il progetto riguardano il superamento dell'attuale frammentazione dei mercati in Europa, la promozione degli investimenti nelle infrastrutture necessarie al pieno sviluppo delle opportunità offerte dalla digitalizzazione e la realizzazione di efficienti sistemi di *e-government*[4].

In questo documento ci concentriamo su due dei temi oggetto delle iniziative europee nell'ambito dell'Agenda digitale: il **quadro giuridico in tema di identificazione e autenticazione on-line** e le misure volte a promuovere la **diffusione di sistemi di pagamento elettronici affidabili ed efficaci**. Anche se i due temi richiedono una trattazione distinta, essi presentano importanti aspetti comuni.

Anzitutto sia l'**identificazione elettronica che i pagamenti elettronici hanno un rilievo trasversale per lo sviluppo dell'economia digitale**. In tutti i rapporti on-line è fondamentale disporre di strumenti che consentano di identificare in via elettronica il soggetto con cui si interagisce in rete. La disponibilità di efficaci canali di pagamento in rete costituisce a sua volta una componente essenziale per tutte le transazioni economiche on-line. Questi due temi hanno quindi un'importanza centrale nella vita dei cittadini e delle imprese: nei rapporti con le amministrazioni pubbliche, nei rapporti tra imprese, nei rapporti tra imprese e consumatori.

Inoltre, sia per l'identificazione che per i pagamenti vi è l'esigenza di mettere a disposizione di cittadini e imprese **strumenti di semplice utilizzo e che assicurino al tempo stesso condizioni di sicurezza adeguate alle diverse esigenze**. La mancanza di sicurezza è infatti uno dei principali fattori che incidono negativamente sullo sviluppo dell'economia digitale.

Infine, in entrambi gli ambiti per sfruttare al meglio le opportunità offerte dalla digitalizzazione occorrono **soluzioni interoperabili**. Per conseguire questo obiettivo le iniziative limitate ai confini nazionali sono insufficienti: occorre un'azione europea volta a rimuovere gli ostacoli alla realizzazione del mercato interno e a promuovere l'interoperabilità a livello globale.

[3] Comunicazione *Un quadro coerente per rafforzare la fiducia nel mercato unico digitale del commercio elettronico e dei servizi* on-line ("comunicazione del 2012 sul commercio elettronico"), cit., pag. 1.
[4] Cfr. Atto per il mercato unico II. In questo senso, si veda anche la risoluzione del Parlamento europeo dell'11 dicembre 2012, 2012/2030/INI.

Proposizione 1 – Gli strumenti di identificazione elettronica e i pagamenti on-line svolgono un ruolo fondamentale per lo sviluppo dell'economia digitale. Per sfruttare appieno le opportunità offerte dalla digitalizzazione occorrono strumenti di semplice utilizzo, con caratteristiche di sicurezza adeguate alle diverse esigenze e interoperabili.

Una questione centrale, in entrambe le aree, è quale debba essere **il ruolo del mercato** e quale **il ruolo della politica pubblica** al fine di fornire a cittadini e imprese l'accesso a strumenti di semplice utilizzo, sicuri e interoperabili. In questi ambiti in cui l'innovazione svolge un ruolo centrale, la **tecnologia** mette a disposizione molte opzioni e la **concorrenza** porta gli operatori a offrire prodotti e servizi sempre più attraenti in termini di qualità e prezzo. I processi di **standardizzazione** sono indispensabili per fare emergere dal mercato un numero circoscritto di soluzioni che siano effettivamente interoperabili. Se i metodi, i sistemi e le interfacce presenti sul mercato sono troppi, infatti, diviene estremamente difficile assicurare l'interoperabilità. La **normativa** svolge un ruolo fondamentale nel chiarire il valore giuridico delle soluzioni messe a disposizione della tecnologia (ad esempio, dei vari sistemi di identificazione elettronica), anche tenendo conto delle loro caratteristiche in termini di sicurezza. Le scelte di politica pubblica possono influire fortemente sullo sviluppo delle soluzioni offerte dal mercato quando impongono per determinate operazioni (ad esempio, per i rapporti dei cittadini e delle imprese con le pubbliche amministrazioni) l'impiego di strumenti che soddisfano determinati requisiti e livelli di sicurezza. Ad esempio, in Italia la firma digitale si è diffusa tra le imprese principalmente in seguito all'introduzione dell'obbligo di utilizzare questo strumento nei rapporti con il Registro delle imprese.

Proposizione 2 – Nei settori innovativi la concorrenza induce gli operatori a sviluppare prodotti e servizi innovativi, di qualità e a prezzi convenienti. I processi di standardizzazione svolgono un ruolo essenziale per assicurare l'interoperabilità delle soluzioni. La normativa contribuisce in misura importante al buon funzionamento del sistema chiarendo quando necessario, ad esempio per gli strumenti di identificazione elettronica, il valore giuridico delle diverse soluzioni.

L'obiettivo di questo lavoro è illustrare le iniziative in corso e formulare alcune considerazioni sulle auspicabili linee di azione da parte delle istituzioni europee e delle autorità nazionali.

1. Identificazione elettronica e firme elettroniche

1.1 Caratteristiche dei processi di identificazione elettronica ed esigenze degli utenti

L'identificabilità dei soggetti e la possibilità di ricondurre ad essi gli atti compiuti attraverso la rete costituiscono aspetti fondamentali della sicurezza delle transazioni su internet. La modalità di autenticazione oggi più diffusa è l'uso di password, ma è evidente la necessità di disporre anche di soluzioni alternative[5].

Per avviare la riflessione sulle caratteristiche del quadro giuridico e di *governance* più appropriato in questo settore è utile ricordare brevemente come sono articolati i sistemi di identificazione on-line[6]. Occorre anzitutto che al soggetto venga attribuita un'identità digitale, ossia una rappresentazione virtuale dell'identità personale che può essere usata durante interazioni con macchine e/o servizi informatici; al soggetto corrisponde quindi un "profilo", costituito da dati identificativi dell'utente, più o meno verificabili. Al soggetto devono essere poi attribuite "credenziali" che permettono la verifica dell'identità da parte del sistema informatico, ossia l'autenticazione. Le credenziali possono essere basate su informazioni a conoscenza del soggetto (come *user-name* e *password*; *one time password* - OTP), oppure corrispondere a determinate caratteristiche fisiche (impronte digitali, iride dell'occhio, firme grafometriche), oppure essere costituite da tessere magnetiche o informazioni poste su un supporto (carta nazionale dei servizi e carta d'identità elettronica). Le credenziali vanno distinte dai supporti che possono essere utilizzati per conservarle, insieme al profilo, e a trasportarle. I supporti sono ad esempio le *smartcard*, i *token* OTP e strumenti quali la combinazione di telefono cellulare e di una sim.

In pratica il processo che porta all'identificazione elettronica avviene in più fasi. Anzitutto, all'utente, previa verifica più o meno rigorosa dell'identità personale, viene attribuita un'identità digitale e viene consegnato un meccanismo per l'autenticazione. Successivamente, il meccanismo deve essere utilizzato ogni volta che si accede al servizio e consente al sistema di verificare in via informatica l'identità del soggetto. Dal punto di vista funzionale occorre distinguere il ruolo dei soggetti che offrono agli utenti funzionalità applicative (*service/application provider*) da quello dei soggetti specializzati nella gestione dell'identità digitale (*identity providers*), che verificano la validità delle credenziali dell'utente e rilasciano le attestazioni di autenticazione.

[5] COM(2010) 245 def., pag. 11.

[6] Su questi temi, rinviamo in particolare ai numerosi lavori del Cefriel. Cfr. ad esempio la presentazione di Alfonso Fuggetta e Massimiliano Pianciamore su "*Identità digitale: riflessioni e sviluppi*", presentata in occasione del convegno Assonime su Identificazione elettronica e sviluppo dell'economia digitale, pubblicata in Note e studi Assonime n. 3 del 3 febbraio 2013.

I diversi modelli di autenticazione differiscono tra loro per livello di **sicurezza**. Oltre alle caratteristiche tecnologiche del processo di autenticazione, un aspetto fondamentale è come avviene l'accertamento dell'effettiva identità dell'utente nella fase iniziale di registrazione. Vi sono sistemi che richiedono la registrazione "*de visu*" allo sportello con documenti verificabili; altri si basano sulla registrazione on-line tramite canali di sicurezza; altri ancora sull'autoregistrazione on-line da parte dell'utente, con verifiche in forma "leggera" o senza alcuna verifica. Un altro aspetto rilevante per la sicurezza è la modalità con cui viene consegnato all'utente il meccanismo di autenticazione: consegna fisica "*brevi manu*" previa presentazione di documento verificabile; invio a recapiti registrati presso fonti ufficiali; attribuzione con doppio canale (ad esempio in parte on-line, in parte tramite sms o invio postale) o attribuzione solo on-line.

Varia peraltro anche la **semplicità di utilizzo** delle credenziali. Alcune credenziali sono meno facilmente spendibili perché richiedono la dotazione di dispositivi specifici (ad esempio, occorre un lettore per la smart card che va configurato sul dispositivo che si vuole utilizzare). Il caso della firma digitale è esemplare: lo strumento, che offre elevate caratteristiche di sicurezza, è ormai ampiamente utilizzato dalle imprese e dai professionisti, con modalità sempre più agevoli (ad esempio, possibilità di firmare in remoto). Esso invece, almeno sino ad oggi, non ha avuto una significativa diffusione tra i consumatori. I costi connessi, in particolare, alla necessità di dotarsi di un dispositivo specifico di firma sono stati presumibilmente ritenuti superiori ai vantaggi dell'utilizzo della firma digitale rispetto a forme alternative di identificazione, anche se meno sicure, per le interazioni on-line.

Proposizione 3 – Il grado di sicurezza richiesto in relazione all'identificazione dell'utente varia in relazione al tipo di operazione che si deve effettuare. Tenendo conto anche del profilo della semplicità di utilizzo della credenziale, non esiste un'unica soluzione adeguata a tutti i contesti. È quindi appropriato che l'utente possa accedere a una pluralità di credenziali, tra loro complementari, da utilizzare in base al requisito di sicurezza dell'operazione.

Ogni soggetto oggi tipicamente ha più identità digitali e utilizza più credenziali per operare on-line. Spesso i singoli servizi hanno propri sistemi di gestione degli utenti. L'attuale frammentazione va oltre quanto giustificato da ragioni di diverso livello di sicurezza dei sistemi di autenticazione. Per semplificare il sistema a vantaggio degli utenti è utile promuovere l'interoperabilità delle credenziali e consentire l'utilizzo di una medesima credenziale su più applicazioni.

L'esigenza di interoperabilità dei sistemi di identificazione si pone sia a livello nazionale sia per le relazioni transfrontaliere. In particolare, all'interno dell'Unione europea per accedere a servizi

di *e-government* o firmare un contratto in un altro Stato membro sia il cittadino che l'impresa spesso si trovano a dovere utilizzare strumenti diversi da quelli previsti nello Stato di origine. Sono in corso a livello europeo e internazionale importanti progetti che hanno come obiettivo proprio quello di consentire, attraverso l'interoperabilità, l'utilizzo degli strumenti di identificazione elettronica al di fuori dei confini nazionali. Tra questi, vanno ricordati in particolare il progetto STORK (Secure Identity AcrossBorders Link) sull'identità elettronica e il progetto PEPPOL (Pan-European Public Procurement On-line), sugli appalti pubblici[7].

Proposizione 4 – Salvaguardando la disponibilità di più credenziali, eterogenee e complementari, per l'accesso alle applicazioni, per semplificare il sistema a vantaggio degli utenti è utile promuovere l'interoperabilità delle credenziali e consentire l'utilizzo di una medesima credenziale su più applicazioni. Per perseguire questo obiettivo, occorre da un lato promuovere l'interoperabilità tecnologica, dall'altro assicurare un quadro giuridico che dia certezza circa la possibilità di utilizzare un determinato sistema di identificazione e autenticazione elettronica per uno specifico obiettivo, ad esempio la partecipazione ad un appalto pubblico.

Nel sistema così configurato è possibile il pieno sviluppo della concorrenza tra i soggetti specializzati nell'offerta di funzionalità applicative agli utenti (*service/application providers).* Anche il servizio di gestione dell'identità digitale (in particolare, verifica della validità delle credenziali e rilascio delle attestazioni di autenticazione) può essere svolto da una pluralità di *identity providers*. L'adozione da parte di questi soggetti di un approccio "federato", basato non solo su standard di interoperabilità tecnologica ma anche su linee guida di tipo tecnico organizzativo, può contribuire a migliorare il funzionamento del settore assicurando la fiducia tra le parti.

Proposizione 5 – Per razionalizzare il funzionamento del settore, è opportuno che sia i *service/application providers*, sia i gestori dell'identità digitale operino secondo un approccio "federato", basato non solo su standard di interoperabilità tecnologica ma anche su linee guida di tipo tecnico-organizzativo volte ad assicurare la fiducia tra le parti. Si potrebbe così arrivare a un sistema integrato, nel quale ogni utente abbia un'unica identità digitale e possa identificarsi on-line attraverso diversi supporti e diversi servizi, con modalità idonee ad assicurare il livello di sicurezza appropriato in relazione alle esigenze dell'operazione che intende effettuare. Resta naturalmente impregiudicata la possibilità per i singoli erogatori di servizi e applicazioni che non intendono aderire al modello federato di continuare a gestire in proprio l'autenticazione degli utenti.

[7] A livello europeo va ricordato anche l'*European Action Plan on e-Signatures and e-Identification* e negli Stati Uniti il progetto IDManagement.gov (Open Identity Solutions for Open Governments).

1.2 Il quadro normativo europeo vigente

Il primo intervento normativo a livello europeo nel settore dell'identificazione elettronica risale a quasi quindici anni fa. La direttiva 1999/93/CE parte dalla constatazione che la divergenza delle norme in tema di riconoscimento giuridico delle firme elettroniche e di accreditamento dei prestatori dei relativi servizi di certificazione negli Stati membri può ostacolare lo sviluppo delle comunicazioni elettroniche e del commercio elettronico e definisce un quadro giuridico comune per agevolare l'uso delle firme elettroniche. A questo fine essa distingue tra la firma elettronica semplice e la firma elettronica avanzata. La firma elettronica semplice è definita come un insieme di dati in forma elettronica allegati oppure connessi tramite associazione logica ad altri dati elettronici e utilizzata come metodo di autenticazione. La firma elettronica avanzata è invece una firma elettronica che soddisfa i seguenti requisiti: è connessa in maniera univoca al firmatario, è idonea a identificarlo, è creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo ed è collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di tali dati. All'interno della categoria delle firme elettroniche avanzate è poi individuato il sottoinsieme delle cosiddette firme elettroniche qualificate: si tratta delle firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura[8]. Va notato che **la distinzione tra le categorie di firma si fonda esclusivamente su requisiti di prestazione/funzionalità, secondo un approccio aperto alle varie tecnologie e ai vari servizi che possono consentire di autenticare i dati in modo elettronico**.

La direttiva 1999/93/CE richiede agli Stati membri di riconoscere determinati effetti giuridici alle firme elettroniche in relazione alle loro caratteristiche. Alle firme elettroniche qualificate deve essere riconosciuto il valore legale di una firma (ossia di una sottoscrizione) in relazione ai dati in forma elettronica così come una firma autografa lo possiede per i dati cartacei; le firme qualificate sono inoltre ammesse come prova in giudizio. Le firme elettroniche (che in quanto tali costituiscono uno strumento di autenticazione, ma non di sottoscrizione) non devono essere considerate legalmente inefficaci o inammissibili come prova in giudizio unicamente per il fatto che sono in forma elettronica, non sono basate su un certificato qualificato o non sono create da un dispositivo per la creazione di una firma sicura.

La direttiva detta alcune regole sui prestatori dei servizi di certificazione volte a consentire lo svolgimento di attività transfrontaliere. La prestazione dei servizi non deve essere soggetta a autorizzazione preventiva. I prestatori di servizi devono inoltre essere liberi di aderire a sistemi

[8] Un certificato qualificato è un attestato elettronico che collega i dati di verifica della firma a una persona e conferma l'identità di tale persona, conforme ai requisiti fissati dall'allegato 1 della direttiva e fornito da un prestatore di servizi di certificazione che soddisfa i requisiti di cui all'allegato 2. Un dispositivo per la creazione di una firma sicura è un software configurato o un hardware utilizzato per applicare i dati per la creazione di una firma che soddisfa i requisiti di cui all'allegato 3 della direttiva.

di accreditamento facoltativo volti ad assicurare gli utenti circa il livello di fiducia, qualità e sicurezza del servizio offerto. Gli Stati sono tenuti a istituire un sistema di supervisione dei prestatori di servizi di certificazione stabiliti nel loro territorio. Sono definite regole comuni circa la responsabilità per eventuali danni causati dai prestatori di servizi e circa gli obblighi che questi devono rispettare per la protezione dei dati personali degli utenti.

Per il funzionamento del mercato interno, la direttiva richiede che ciascuno Stato membro applichi le disposizioni attuative della direttiva ai prestatori di servizi stabiliti nel suo territorio e ai servizi da essi forniti, e non limiti la prestazione di servizi di certificazione originati in un altro Stato membro. Inoltre, deve essere consentito ai prodotti di firma elettronica conformi alla direttiva di circolare liberamente nel mercato interno.

La direttiva contiene una regola particolare per il settore pubblico (c.d. *public sector clause*): agli Stati è consentito assoggettare l'uso delle firme elettroniche nel settore pubblico a eventuali requisiti supplementari, purché obiettivi, trasparenti, proporzionati e non discriminatori.

Per quanto riguarda il rapporto con gli standard, la direttiva prevede che la Commissione possa determinare e pubblicare i numeri di riferimento di standard generalmente riconosciuti relativi a prodotti di firma elettronica. Prodotti di firma elettronica che rispettano tali standard armonizzati sono considerati conformi ai requisiti di cui agli allegati della direttiva[9].

La Commissione è assistita da un comitato di rappresentanti degli Stati membri che ha il compito di precisare alcuni profili della disciplina (ad esempio, i requisiti indicati negli allegati).

Riguardo ai profili internazionali, la direttiva definisce i requisiti che devono essere soddisfatti perché i certificati qualificati rilasciati da un prestatore di servizi stabilito in un paese terzo siano riconosciuti come equivalenti a quelli di un prestatore stabilito nella Comunità e indica le iniziative che la Commissione può adottare per agevolare servizi di certificazione transfrontalieri con paesi terzi e il riconoscimento giuridico delle firme elettroniche avanzate che hanno origine in paesi terzi (attuazione di norme e accordi internazionali esistenti, proposte al Consiglio di negoziazione di nuovi accordi bilaterali e multilaterali).

La direttiva è stata recepita in tutti gli Stati membri. In Italia le norme di recepimento, ripetutamente riviste, sono contenute nel decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale - CAD).

[9] In particolare, ai requisiti dell'allegato 2, lettera f, e dell'allegato 3.

Proposizione 6 – L'approccio della disciplina europea delle firme elettroniche contenuta nella direttiva 1999/93/CE presenta importanti caratteristiche positive: si basa su nozioni neutrali sotto il profilo tecnologico, prevede l'obbligo per gli Stati membri di riconoscere (almeno) un determinato valore giuridico a determinate soluzioni, collega la disciplina agli standard armonizzati progressivamente pubblicati dalla Commissione, sancisce i principi di libera circolazione dei servizi e dei prodotti, istituisce meccanismi di accreditamento e supervisione per assicurare la fiducia in relazione ai servizi di certificazione.

Dall'esperienza relativa all'applicazione della direttiva sono però emerse alcune carenze:

a) la direttiva si occupa principalmente della firma elettronica qualificata quale strumento di sottoscrizione, e dei relativi servizi di certificazione, trascurando altri profili che sono essenziali per il buon funzionamento delle comunicazioni elettroniche e del commercio elettronico nell'Unione europea. Molte transazioni elettroniche infatti non richiedono una sottoscrizione, ma richiedono l'identificazione del soggetto ed eventualmente altre funzionalità (la garanzia di non modificazione del contenuto del documento; la certezza sulle date di invio e ricezione e così via). La direttiva non pone alcuna regola comune su questioni importanti quali il valore giuridico del documento informatico, i servizi elettronici di recapito, le marche temporali ecc;
b) vi sono state interpretazioni divergenti delle disposizioni della direttiva e gli standard tecnici sono stati applicati in modo non uniforme a livello nazionale, pregiudicando l'interoperabilità delle soluzioni;
c) le disposizioni in tema di supervisione sono state attuate in modo disomogeneo tra Stati membri, con effetti negativi sulla fiducia reciproca;
d) la regola speciale per il settore pubblico ha portato all'adozione negli Stati membri di requisiti di identificazione per l'accesso ai servizi pubblici che ostacolano l'accesso da parte di soggetti di altri Stati membri.

Per questo la Commissione europea ha ritenuto di procedere a una revisione della direttiva sulle firme elettroniche, volta ad assicurare anche il mutuo riconoscimento dei sistemi di identificazione elettronica e a istituire un quadro normativo per il riconoscimento e l'interoperabilità transfrontalieri di sistemi di autenticazione elettronica sicuri[10].

[10] Cfr. le azioni fondamentali 3 e 16 dell'Agenda digitale europea, COM(2010)245; cfr. anche l'Atto per il mercato unico, COM(2011)206, pp. 12-14.

1.3 La proposta di regolamento sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno

Nel giugno 2012 la Commissione ha presentato una proposta di regolamento del Parlamento europeo e del Consiglio "sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno", che dovrebbe sostituire la direttiva 1999/93/CE. Trattandosi di un regolamento, e non di una direttiva, le disposizioni saranno direttamente applicabili negli Stati membri; ciò dovrebbe ridurre il rischio di applicazioni eterogenee negli Stati membri.

L'ambito di applicazione è molto più ampio di quello della precedente direttiva: esso copre infatti identificazione elettronica, firme elettroniche, sigilli elettronici per le persone giuridiche, validazione temporale elettronica, documenti elettronici, servizi elettronici di recapito, autenticazione dei siti web. L'obiettivo è favorire il mutuo riconoscimento e l'accettazione all'interno dell'Unione europea degli schemi di identificazione elettronica e di altri servizi elettronici fiduciari ausiliari.

Gli Stati membri restano liberi di decidere se adottare strumenti di identificazione elettronica per i cittadini (ad esempio, carte di identità elettroniche) e possono legittimamente promuovere la diffusione di determinati strumenti (ad esempio richiedendo per certi adempimenti l'utilizzo della firma digitale o della posta elettronica certificata). Ma per poter cogliere i frutti economici e sociali della digitalizzazione occorre che gli strumenti adottati a livello nazionale consentano di operare *cross border* in tutti gli Stati membri. La giustificazione dell'intervento europeo è che le misure adottate a livello nazionale non sono adeguate ad assicurare l'interoperabilità delle soluzioni; inoltre, per creare la fiducia necessaria per il buon funzionamento del sistema occorre rafforzare il coordinamento dei regimi nazionali di supervisione sui prestatori di servizi fiduciari.

Il progetto di regolamento europeo sottolinea l'obiettivo di un mercato integrato in cui le imprese possano partecipare on-line agli appalti pubblici in altri Stati membri, rimuovendo gli ostacoli connessi alla mancata accettazione o all'assenza di interoperabilità degli strumenti di sottoscrizione della domanda.

Similmente, il quadro giuridico europeo dovrebbe consentire di stipulare contratti on-line con imprese di altri Stati membri senza incertezze riguardo al valore di documenti elettronici, marche temporali e così via. Le imprese dovrebbero poter utilizzare gli "sportelli unici" previsti dalla direttiva servizi per le pratiche amministrative nei vari Stati membri senza ostacoli connessi a requisiti idiosincratici di identificazione, autenticazione e firma elettronica. I cittadini dovrebbero poter impiegare al di fuori dei confini nazionali gli strumenti di identificazione elettronica accettati nel proprio paese di origine, ad esempio per iscriversi on-line a un'università o accedere al proprio fascicolo elettronico se intendono avvalersi di servizi sanitari in un altro Stato membro.

Proposizione 7 – Come nel settore della protezione dei dati personali, anche nel settore dell'identificazione e dell'autenticazione elettronica l'adozione di un regolamento, invece di una direttiva, può contribuire ad assicurare un'applicazione più uniforme negli Stati membri. L'ampliamento dell'ambito di applicazione della normativa europea, rispetto a quello della direttiva sulle firme elettroniche, appare appropriato per favorire l'utilizzo transfrontaliero di una serie di strumenti importanti per la realizzazione delle transazioni on-line.

Mutuo riconoscimento dell'identificazione elettronica

Il progetto di regolamento lascia impregiudicata la libertà degli Stati membri di stabilire quali strumenti di identificazione elettronica utilizzare per l'accesso ai servizi on-line nel proprio territorio. Viene però sancito l'obbligo di assicurare il mutuo riconoscimento e l'accettazione delle soluzioni adottate in altri Stati e notificate alla Commissione. Più precisamente, quando uno Stato membro prevede l'identificazione elettronica del soggetto per dare l'accesso ad alcuni servizi pubblici on-line deve assicurare il mutuo riconoscimento degli schemi di identificazione elettronica utilizzati in altri Stati membri per concedere l'accesso on-line ai servizi pubblici.

Per ottenere il mutuo riconoscimento, gli schemi degli altri Stati devono essere stati **notificati alla Commissione europea** e soddisfare certi **requisiti** (in particolare, lo strumento di identificazione elettronica deve essere emesso sotto la responsabilità dello Stato che notifica lo schema; lo Stato deve assicurare un legame certo tra i dati di identificazione elettronica e il soggetto; deve essere possibile per il soggetto di un altro Stato membro accedere gratuitamente on-line all'autenticazione dei dati).

Gli schemi di identificazione elettronica notificati dagli Stati membri saranno pubblicati dalla Commissione europea in un apposito elenco.

Gli Stati membri sono tenuti a cooperare per assicurare l'interoperabilità degli strumenti di identificazione che rientrano in un regime notificato e rafforzarne la sicurezza. La Commissione adotterà le misure attuative e gli atti delegati utili a facilitare la cooperazione tra Stati membri, anche fissando requisiti minimi a livello tecnologico.

Ciascuno Stato membro potrà inoltre valutare se estendere anche al settore privato l'utilizzo degli strumenti di identificazione "notificati".

Va sottolineato che l'identificazione elettronica è intesa, in questo contesto, come l'utilizzo dei dati in forma elettronica che identificano senza ambiguità una persona fisica o giuridica. Il legame non ambiguo tra i dati di identificazione e il soggetto sarà tipicamente assicurato da un sistema di autenticazione a due fattori (ciò che possiedo e ciò che conosco). Gli strumenti di

identificazione possono essere ad esempio carte d'identità elettroniche, ma anche chiavette, carte SIM dei telefoni, carte bancarie, patenti di guida o carte sanitarie elettroniche, combinazioni di *user-id* e *password* e così via. Il progetto di regolamento non interferisce con le scelte tecnologiche e si limita a chiedere agli Stati di cooperare per assicurare l'interoperabilità degli strumenti di identificazione inclusi in schemi notificati e per rafforzare la loro sicurezza.

Proposizione 8 – La proposta relativa al mutuo riconoscimento degli schemi di identificazione elettronica utilizzati dagli Stati membri per l'accesso ai servizi pubblici e notificati alla Commissione, accompagnata da iniziative volte ad assicurare l'interoperabilità e la sicurezza di tali schemi, può favorire l'accesso transfrontaliero on-line ai servizi pubblici da parte di cittadini e imprese. Le soluzioni che si affermeranno a livello europeo per l'accesso ai servizi pubblici facilmente troveranno utilizzo anche nelle transazioni tra privati.

Quadro giuridico per i servizi di certificazione on-line

Il progetto di regolamento fissa alcuni obblighi per la prestazione di servizi di certificazione elettronica, in particolare per i servizi di certificazione qualificati. È fissato l'obbligo di adottare le misure tecniche e organizzative appropriate per assicurare un livello di sicurezza proporzionato ai servizi fiduciari offerti e quello di notificare alle autorità eventuali violazioni della sicurezza. È disciplinata la responsabilità in caso di danni derivanti dal mancato rispetto degli obblighi previsti dal regolamento e sono rafforzati i vincoli in materia di protezione dei dati personali e minimizzazione dell'utilizzo di tali dati.

I sistemi di vigilanza a livello nazionale sono armonizzati e sensibilmente rafforzati ed è prevista la cooperazione tra le autorità di vigilanza dei diversi Stati per favorire il mutuo riconoscimento e l'utilizzo transfrontaliero di tali servizi.

Per i servizi di certificazione forniti extra UE il compito di assicurare il mutuo riconoscimento è demandato ad accordi tra l'Unione europea e paesi terzi; tali accordi devono assicurare che il prestatore rispetti i requisiti relativi alla protezione dei dati, alla sicurezza e alla vigilanza previsti nell'Unione europea.

Gli Stati membri sono tenuti a pubblicare liste dei fornitori di servizi fiduciari elettronici qualificati, che devono includere informazioni sui servizi forniti (*trusted lists*). Per i servizi fiduciari qualificati è previsto il mutuo riconoscimento. I requisiti che devono essere soddisfatti dai fornitori di servizi qualificati sono indicati nel regolamento e potranno essere ulteriormente specificati dalla Commissione, attraverso misure attuative, che prevedano il riferimento a determinati standard relativi a sistemi e prodotti sicuri. L'utilizzo di tali standard comporta la presunzione che siano soddisfatti i requisiti previsti dal regolamento.

Proposizione 9 – La precisazione degli obblighi che devono essere soddisfatti dai prestatori di servizi di certificazione qualificati e il rafforzamento dei sistemi di vigilanza appaiono utili per accrescere la fiducia nei servizi offerti e quindi incentivare l'utilizzo degli strumenti elettronici contemplati dal regolamento.

Firme elettroniche

Il progetto di regolamento apporta alcuni chiarimenti alle definizioni di firme elettroniche (che includono le firme "in remoto/tramite server" e quelle realizzate con dispositivo mobile). Viene anzitutto chiarita la distinzione tra firma e identificazione elettronica: la firma elettronica è utilizzata per firmare, va distinta sul piano logico dagli strumenti utilizzabili per identificarsi in rete (anche se in concreto un medesimo strumento, ad esempio una firma digitale, può essere impiegata per entrambi i fini). La firma elettronica, come la firma autografa, riguarda solo le persone fisiche.

L'effetto giuridico delle diverse tipologie di firma è il medesimo previsto dalla direttiva: alla firma elettronica semplice non può essere negato di per sé valore giuridico o ammissibilità come prova in giudizio solo per il fatto di essere in forma elettronica; la firma elettronica qualificata ha un valore giuridico equivalente a quello di una firma autografa e deve essere riconosciuta e accettata in tutti gli Stati membri. Un'importante novità, rispetto alla direttiva, è che gli Stati membri non possono chiedere per l'accesso transfrontaliero a un servizio on-line un livello di sicurezza più elevato di quello di una firma elettronica qualificata. Ciò significa, ad esempio, che non potrà essere imposto l'utilizzo della firma digitale come unica soluzione.

La Commissione potrà adottare atti delegati per specificare i diversi livelli di sicurezza delle firme elettroniche. Se per accedere a un servizio pubblico on-line uno Stato membro richiede una firma con livello di sicurezza inferiore alla firma qualificata, deve riconoscere e accettare tutte le firme che raggiungono almeno lo stesso livello di sicurezza. La Commissione con misure attuative potrà indicare i numeri di riferimento di standard relativi ai diversi livelli di sicurezza. Se la firma è basata sullo standard armonizzato, si presume che soddisfi il corrispondente livello di sicurezza.

Gli strumenti per la creazione di firme qualificate possono essere certificati e in tal caso dovranno essere notificati alla Commissione. La Commissione pubblicherà e terrà aggiornata una lista degli strumenti certificati per la creazione di firme elettroniche qualificate.

La proposta di regolamento inoltre chiarisce i requisiti per la convalida della firma qualificata e richiede che il servizio di conservazione delle firme qualificate fornito da prestatori di servizi

qualificati sia svolto con procedure e tecnologie in grado di estendere l'affidabilità dei dati di convalida della firme oltre il periodo di validità tecnologica.

E-seals e validazione temporale

Per le persone giuridiche sono previsti sigilli elettronici (*electronic seals)* che assicurano l'origine e l'integrità del documento e attestano la sua provenienza dalla persona giuridica. Anche ai sigilli elettronici non può essere negato valore giuridico e ammissibilità come prova in giudizio per il solo fatto di essere in forma elettronica. Per i sigilli elettronici qualificati è previsto il mutuo riconoscimento. Inoltre, in analogia a quanto previsto per le firme, uno Stato membro non può richiedere per l'accesso a servizi pubblici on-line un sigillo elettronico con livello di sicurezza superiore a quello di un sigillo elettronico qualificato; quando uno Stato membro accetta per l'accesso a un servizio pubblico on-line un sigillo con livello di sicurezza inferiore a quello qualificato, deve accettare anche altre soluzioni che soddisfino lo stesso livello di sicurezza. Anche per i sigilli qualificati, come per le firme qualificate, sono previste disposizioni sugli strumenti sicuri per la creazione del sigillo, che possono essere certificati e pubblicati, nonché sulla convalida e la conservazione della validità. Nelle transazioni che richiedono il sigillo elettronico certificato deve essere accettata, in alternativa, la firma qualificata del rappresentante autorizzato della persona giuridica.

Analogamente, il progetto di regolamento disciplina l'effetto giuridico della validazione temporale elettronica e individua alcuni requisiti per la validazione temporale elettronica qualificata, per la quale è previsto il mutuo riconoscimento.

L'apposizione della validazione temporale elettronica comporta la presunzione legale di garanzia dell'ora e della data che sono indicate e dell'integrità dei dati a cui l'ora e la data sono associate.

Documenti elettronici

Una delle principali novità del regolamento è l'indicazione sul valore giuridico dei documenti elettronici. In Italia esistono da tempo disposizioni in tal senso[11], ma mancava sinora una disciplina uniforme tra gli Stati membri.

Il progetto di regolamento sancisce il principio di non discriminazione tra documenti cartacei e elettronici: un documento elettronico sarà considerato equivalente a un documento cartaceo e ammissibile come prova in giudizio tenuto conto del livello di sicurezza circa la provenienza e l'integrità del contenuto. Per i documenti elettronici a cui sono apposti una firma elettronica qualificata o un sigillo elettronico qualificato vi è la presunzione di autenticità e integrità del

[11] Articoli 20 e 21 del CAD.

contenuto (a condizione che il documento non abbia caratteristiche dinamiche in grado di modificarlo automaticamente). Quando per l'accesso a un servizio pubblico è richiesto un documento originale o una copia certificata, i documenti elettronici che nello Stato membro di origine sono considerati originali o copie certificate devono essere accettati come tali anche negli altri Stati membri, senza requisiti addizionali.

Servizi elettronici di recapito

Nel progetto di regolamento viene disciplinato per la prima volta a livello europeo il valore giuridico dei servizi elettronici di recapito, intesi come quei servizi che rendono possibile la trasmissione dei dati per via elettronica, forniscono evidenza sulla gestione della trasmissione (tra cui vi è la prova dell'invio e della consegna) e proteggono l'integrità del contenuto. I dati trasmessi o ricevuti utilizzando un servizio elettronico di recapito sono ammissibili come prova in giudizio per quanto riguarda l'integrità dei dati e la certezza dell'ora e della data, dell'invio e della ricezione.

Per i servizi elettronici di recapito qualificati (che devono soddisfare i requisiti indicati nel regolamento) è previsto il mutuo riconoscimento e vi è la presunzione legale di integrità dei dati e di accuratezza dell'ora e della data di invio e consegna. La Commissione è incaricata di promuovere l'interoperabilità delle soluzioni.

Autenticazione dei siti

Infine il progetto di regolamento prevede che possano essere rilasciati certificati qualificati che consentono di autenticare un sito web e collegano il sito alla persona a cui il certificato è rilasciato. I certificati qualificati di autenticità del sito, dei quali il regolamento specifica i requisiti, dovranno essere riconosciuti e accettati in tutti gli Stati membri.

Proposizione 10 – L'indicazione in un regolamento europeo del valore giuridico dei vari strumenti utilizzabili nelle transazioni on-line e dei requisiti che devono essere soddisfatti per ottenere il mutuo riconoscimento costituisce un contributo fondamentale per il funzionamento del mercato interno digitale.

Proposizione 11 – La disponibilità di sistemi di certificazione dell'autenticità dei siti che soddisfano requisiti fissati a livello europeo e per i quali è previsto il mutuo riconoscimento risponde all'esigenza degli utenti di fiducia circa l'identità dei soggetti con cui interagiscono in rete e può contribuire in misura importante allo sviluppo delle transazioni elettroniche.

Rapporto tra legislazione e sviluppo delle soluzioni tecnologiche e organizzative

Per non cristallizzare eccessivamente la disciplina all'interno del regolamento, il progetto prevede che la Commissione adotti un ampio numero di atti delegati, ad esempio per fissare i requisiti minimi di sicurezza[12]. Altre misure di attuazione (*implementing acts*) saranno adottate dalla Commissione con l'assistenza di un comitato di rappresentanti degli Stati membri secondo le procedure previste dal regolamento (UE) n. 182/2011[13].

Proposizione 12 – Una struttura a più livelli, basata su regole fissate a livello legislativo e regole attuative più facilmente modificabili, è necessaria per consentire la flessibilità della disciplina in relazione agli sviluppi del mercato; occorre naturalmente trovare, per le diverse questioni, il giusto equilibrio tra regole fissate nel regolamento e le misure delegate o attuative di livello inferiore.

Attraverso le misure attuative la Commissione può indicare i numeri di riferimento di standard tecnici. Per i prodotti e i sistemi basati su questi standard vi sarà la presunzione di conformità ai requisiti indicati dalla disciplina. Ciò non pregiudica la possibilità di soddisfare tali requisiti anche con modalità diverse.

Proposizione 13 – Per favorire l'interoperabilità delle soluzioni è essenziale la definizione di standard tecnici a livello europeo o internazionale che consentano di canalizzare gli sforzi innovativi (ad esempio, sulla rappresentazione delle credenziali utente, sui protocolli d'interazione, sulle modalità di integrazione con le soluzioni esistenti). Secondo le linee della politica europea in tema di standardizzazione, è opportuno che gli standard siano elaborati secondo un processo trasparente, tenendo conto delle osservazioni di tutti i potenziali interessati, e siano accessibili alle imprese che intendono operare nel mercato a valle.

Dal 1° gennaio 2013 è operativo il regolamento (UE) n. 1025/2012 sulla standardizzazione europea che ha modernizzato per alcuni aspetti la politica europea di standardizzazione (sul tema, cfr. il Note e studi Assonime n. 1/2013). Uno degli obiettivi principali della disciplina è velocizzare il processo di adozione degli standard.

[12] Il progetto di regolamento prevede un forte potere di controllo sugli atti delegati della Commissione da parte del Parlamento europeo e del Consiglio. La Commissione dovrà notificare al Parlamento europeo e al Consiglio gli atti delegati e questi ultimi entreranno in vigore solo se non vi sarà opposizione, entro sessanta giorni, da parte di una delle due istituzioni.

[13] Cfr. regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio del 16 febbraio 2011.

Proposizione 14 – L'obiettivo di velocizzare il processo di adozione degli standard, perseguito dal recente regolamento (UE) n. 1025/2012 sulla standardizzazione europea, è fondamentale in settori in rapida evoluzione come quello dell'identificazione elettronica. Una delle criticità riscontrate nel settore, infatti, è la lentezza dell'adeguamento degli standard.

Il progetto di regolamento nel contesto internazionale

Occorre che il progetto europeo sia disegnato tenendo conto degli sviluppi in tema di identificazione on-line al di fuori dell'UE. Il problema di costruire un adeguato quadro giuridico per le transazioni on-line non può essere affrontato solo a livello europeo, occorre una prospettiva globale. Occorre tenere conto, ad esempio, dei lavori dell'UNCITRAL in tema di commercio elettronico[14]. Negli Stati Uniti il punto di riferimento è la US *National Strategy for Trusted Identities in Cyberspace*, basata sull'idea di un ecosistema dell'identità inteso come un "contesto on-line in cui individui e organizzazioni possono fidarsi reciprocamente perché seguono standard condivisi per ottenere e autenticare le loro identità digitali".

Proposizione 15 – L'adozione di una disciplina volta ad assicurare il mutuo riconoscimento e l'interoperabilità all'interno dell'Unione europea non è sufficiente a consentire lo sviluppo di tutte le potenzialità offerte dalle transazioni elettroniche. Occorre che l'Unione europea continui ad agire a livello internazionale, attraverso gli opportuni accordi, per ampliare l'area di mercato in cui vi è interoperabilità e mutuo riconoscimento delle soluzioni.

1.4 L'impatto della nuova disciplina europea: quali sfide per l'Italia

Molti degli ambiti disciplinati dal progetto di regolamento sono già oggetto in Italia di disposizioni normative, oggi raccolte nel Codice dell'amministrazione digitale (CAD). L'Italia per alcuni aspetti è stata un precursore del quadro normativo che sta emergendo a livello europeo; ad esempio, già la legge 15 maggio 1997, n. 59 riconosceva il valore giuridico del documento informatico.

Per quanto riguarda le firme elettroniche, il CAD fa riferimento a tutte le categorie previste dal diritto europeo (firma elettronica semplice, avanzata e qualificata). Sinora nel nostro ordinamento si è dato un forte impulso alla diffusione della firma digitale, che è una tipologia particolare di firma qualificata basata sulla crittografia asimmetrica. Come già accennato, la diffusione della firma digitale è stata promossa prevedendone l'utilizzo obbligatorio in alcuni

[14]Cfr. ad esempio la *UN Convention on the Use of Electronic Communications in International Contracts* del 2005.

rapporti con il settore pubblico (ad esempio, nei rapporti con il Registro delle imprese). La firma digitale ormai è ampiamente utilizzata dalle imprese e dai professionisti.

Sino alla recente adozione delle regole tecniche previste dal CAD, avvenuta con il decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013[15], la diffusione delle firme avanzate e in particolare delle firme qualificate diverse dalla firma digitale è stata rallentata dalle incertezze circa il valore giuridico delle diverse soluzioni.[16]. Occorre ricordare, al riguardo, che le firme elettroniche non sono semplici strumenti, bensì processi che coinvolgono sia profili tecnologici che profili organizzativi ed è indispensabile che siano chiari i requisiti da soddisfare[17]. In questi anni le banche e le imprese hanno comunque fatto un ampio ricorso a forme di firma elettronica avanzata, ma in generale in Italia è rimasto un gap tra le potenzialità offerte dalle nuove tecnologie e quello che realmente si fa e si usa.

Le bozze delle regole tecniche sulle firme erano state pubblicate nel 2011, insieme a bozze di regole tecniche su documento informatico, conservazione e protocollo informatico. Queste ultime regole tecniche sono ancora in attesa di essere emanate.

Proposizione 16 – Le regole tecniche previste dal Codice dell'amministrazione digitale sono essenziali per comprendere il valore giuridico delle varie soluzioni messe a disposizione dal mercato e poterle quindi concretamente utilizzare. Dopo l'adozione delle regole tecniche sulle firme elettroniche occorre procedere rapidamente ad adottare le regole tecniche sul documento informatico, la conservazione, la gestione dei flussi documentali e del protocollo informatico.

Il ritardo nell'adozione delle regole tecniche è in gran parte imputabile alla *governance* della politica pubblica in materia di digitalizzazione nel nostro paese, con competenze frammentate tra diversi Ministeri. Di questa frammentazione sono evidenza anche le perduranti discrasie delle disposizioni del decreto ministeriale sulla conservazione dei documenti in materia fiscale (decreto ministeriale 23 gennaio 2004) rispetto alle disposizioni del CAD.

A questo riguardo recentemente sono state introdotte alcune norme che potenziano l'Agenda digitale italiana intervenendo sulla sua *governance*. In particolare oltre a ridefinire la composizione della cabina di regia dell'Agenda digitale presieduta dal Presidente del Consiglio, viene istituito presso la Presidenza del Consiglio dei ministri "un tavolo permanente per

[15]Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013, pubblicato nella Gazzetta ufficiale n. 117 del 21 maggio 2013 sono state adottate le regole tecniche "in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali". Sono incluse nel decreto le regole per la validazione temporale mediante marca temporale.

[16] Sul tema, cfr. anche gli Stati generali della memoria digitale del marzo 2013, in www.anorc.it, e il Manifesto per l'Italia digitale del 15 aprile 2013.

[17] Giusella Finocchiaro, "Nuova firma per le scritture private", Il Sole 24 Ore, 23 maggio 2013.

l'innovazione e l'agenda digitale italiana", composto da esperti e rappresentanti di imprese e presieduto dal nuovo commissario del governo per l'attuazione dell'Agenda digitale. Le funzioni di vigilanza sull'Agenzia per l'Italia digitale sono attribuite alla Presidenza del Consiglio dei Ministri[18].

È stata anche introdotta una procedura accelerata per l'approvazione delle misure attuative non ancora adottate in materia ad esempio di anagrafe informatizzata della popolazione, censimento della popolazione, pagamenti elettronici, sistemi di bigliettazione elettronica, identificazione delle banche dati di interesse nazionale, domicilio digitale. Se non approvate tempestivamente, queste misure potranno essere adottate dal Presidente del Consiglio dei Ministri.

Proposizione 17- Occorre una *governance* più incisiva delle politiche nazionali in materia di digitalizzazione. È quindi essenziale che il disegno organizzativo incentrato sul rafforzamento delle competenze della Presidenza del Consiglio prenda corpo e dimostri di essere funzionante.

Per quanto concerne gli strumenti di identificazione elettronica, molte pubbliche amministrazioni utilizzano sistemi basati su *username* e *password*. Le carte d'identità elettroniche e le carte nazionali dei servizi sono tuttora poco diffuse. Nel decreto legge 18 ottobre 2012, n. 179, che contiene varie disposizioni sull'agenda digitale italiana, è previsto l'ampliamento delle possibili utilizzazioni della carta d'identità elettronica e la sua unificazione con la tessera sanitaria. Ciò avverrà attraverso un decreto del Presidente del Consiglio dei Ministri[19]; le modalità tecniche per la produzione e gestione del documento unificato dovranno essere fissate con un decreto interministeriale.

L'utilizzo dei dati biometrici come strumento idoneo ad assicurare un elevato livello di sicurezza nell'identificazione elettronica sinora è stato ostacolato da preoccupazioni connesse alla tutela dei dati personali. A questo riguardo, il Garante per la privacy si è espresso su due specifiche richieste di verifica preliminare avanzate da istituti bancari[20]. Le banche volevano rendere disponibile alla clientela un servizio di sottoscrizione dei documenti con firma digitale basato su una procedura di autenticazione biometrica effettuata attraverso il tablet. Il sistema raccoglie le caratteristiche biometriche di natura comportamentale del cliente rilevando e analizzando alcuni parametri (velocità, pressione, ecc.) relativi alla sua firma autografa per confrontarli con quelli

[18] Articolo 13, decreto legge 21 giugno 2013, n. 69, convertito con modificazioni dalla legge 9 agosto 2013, n. 98.
[19] Il Garante per la privacy con il provvedimento n. 39 del 31 gennaio 2013, ha espresso parere favorevole sullo schema di decreto del Presidente del Consiglio volto all'accorpamento della carta d'identità elettronica con la tessera sanitaria in un unico documento digitale.
[20] Provvedimenti del Garante per la privacy n. 36 e 37 del 31 gennaio 2013.

precedentemente memorizzati in fase di adesione al servizio. La comparazione positiva che determina l'autenticazione dell'utente consente l'avvio della procedura di sottoscrizione con firma digitale del documento da parte del cliente. La verifica preliminare presentata all'Autorità dalle due banche aveva ad oggetto la valutazione di conformità del trattamento di dati biometrici dei clienti nella fase di autenticazione alla disciplina del codice privacy. Il Garante ha ammesso il trattamento dei dati biometrici nei due casi, specificando le condizioni che devono essere rispettate.

Da ultimo, il Garante per la privacy si è espresso favorevolmente sulla richiesta di verifica preliminare presentata da una banca sul trattamento dei dati personali connesso all'utilizzo del sistema di firma grafometrica per la sottoscrizione in formato elettronico di atti, contratti e documenti relativi a prodotti e servizi offerti dalla banca, indicando una serie di condizioni integrative da rispettare in tema di sicurezza[21].

Un tema diverso è quello relativo all'individuazione dei casi in cui una firma biometrica possa essere considerata una firma elettronica avanzata ai sensi del CAD. A questo riguardo sono fondamentali le regole tecniche emanate di recente che disciplinano i requisiti della firma elettronica avanzata. Nel caso in cui questi requisiti non vengano rispettati, la firma biometrica costituisce una firma elettronica semplice.

Proposizione 18 – L'utilizzo dei dati biometrici può costituire uno strumento prezioso per l'identificazione sicura dei soggetti nelle transazioni elettroniche. Occorre trovare soluzioni idonee ad assicurare un adeguato livello di tutela dei dati personali senza ostacolare ingiustificatamente lo sviluppo di soluzioni basate sull'impiego di tali dati.

Negli ultimi anni in Italia è stato dato un forte impulso all'utilizzo della posta elettronica certificata, anche se il CAD prevede la possibilità di soluzioni tecnologiche alternative per i servizi di recapito elettronico. La normativa italiana ha progressivamente imposto l'obbligo di dotarsi di un indirizzo PEC per interagire con le pubbliche amministrazioni a società, professionisti e, da ultimo, alle imprese individuali (che devono comunicare l'indirizzo al registro delle imprese entro il 30 giugno 2013). È stato istituito un Indice nazionale degli indirizzi PEC di imprese e professionisti. Per i cittadini invece dotarsi di un indirizzo PEC è facoltativo. Per quelli

[21] Provvedimento del Garante per la privacy n. 396 del 12 settembre 2013. Tra le condizioni imposte dal Garante vi sono: l'adozione di idonee misure volte a ridurre i rischi di installazione abusiva di software o di modificazione della configurazione dei dispositivi in dotazione ai promotori e di ogni altro accorgimento utile a contrastare l'azione di eventuali agenti malevoli; un sistema di gestione dei dispositivi impiegati nei trattamenti grafometrici basato su certificati digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni del loro utilizzo sicuro (inclusa la possibilità di cancellare da remoto in caso di smarrimento o sottrazione dei dispositivi); l'adozione di adeguate poicy per la gestione degli incidenti di sicurezza nell'ambito delle varie fasi del processo biometrico/grafometrico.

che dichiarano un indirizzo PEC, dal 1° gennaio 2013 vi è l'obbligo per le pubbliche amministrazioni e i gestori di pubblici servizi di comunicare esclusivamente al domicilio digitale[22].

Una questione delicata è verificare se la PEC, su cui il nostro sistema ha investito molto, possa in prospettiva affermarsi come soluzione interoperabile a livello europeo. Va osservato che per soddisfare i requisiti previsti dal progetto di regolamento per i servizi di consegna elettronica qualificata, occorre che i servizi di posta elettronica certificata garantiscano anche l'integrità del contenuto del messaggio.

Le disposizioni del Codice dell'amministrazione digitale dovranno essere riviste per adeguarle al nuovo regolamento europeo oggi all'esame del Parlamento europeo e del Consiglio. Anche se il regolamento prevederà un adeguato periodo transitorio, già da ora negli Stati membri occorre attivarsi per effettuare una tempestiva analisi dell'impatto della nuova disciplina su ciascun ordinamento nazionale. In particolare, le scelte strategiche riguardo alla promozione degli strumenti di identificazione e autenticazione on-line devono tenere conto di quello che, in prospettiva, costituirà il quadro di riferimento a livello europeo e dell'esigenza di assicurare soluzioni interoperabili. Un primo passo potenzialmente utile, in questa prospettiva, è la recente istituzione del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), volta a semplificare e rendere più sicura l'interazione con la pubblica amministrazione. Il sistema si configurerà come un insieme aperto di soggetti pubblici e privati che, previo accreditamento, gestiscono i servizi di registrazione e messa a disposizione delle credenziali e degli strumenti di accesso in rete per conto delle pubbliche amministrazioni o direttamente su richiesta degli interessati[23].

Proposizione 19 – Occorre che le amministrazioni italiane partecipino attivamente ai lavori di definizione della disciplina europea, sia nella fase della adozione del regolamento che nella successiva fase dell'adozione delle misure attuative. Bisogna essere ben consapevoli del quadro giuridico che si prospetta, per indirizzare da subito le scelte di *policy* in direzioni conformi al futuro diritto europeo. Un ruolo centrale può essere svolto, in questo contesto, dall'Agenzia per l'Italia digitale.

[22] Le modalità di comunicazione, variazione e cancellazione del proprio domicilio digitale da parte del cittadino devono essere fissate da un decreto ministeriale, ad oggi non emanato. Nell'assetto normativo precedente era stato emanato il decreto del Presidente del Consiglio dei ministri 6 maggio 2009 che reca disposizioni in materia di rilascio e di uso della casella di posta elettronica assegnata ai cittadini (collegato all'articolo 16 bis del decreto legge n. 185/2008).

[23] Articolo 17 ter del decreto legge 21 giugno 2013, n. 69, convertito con modificazioni dalla legge 9 agosto 2013, n. 98.

Un'ulteriore misura che può avere un forte impatto positivo in termini di modernizzazione e semplificazione dei rapporti con le pubbliche amministrazioni è l'istituzione dell'**Anagrafe nazionale della popolazione residente** (ANPR) presso il Ministero dell'interno. La realizzazione della nuova Anagrafe è stata giustamente individuata come prioritaria dal Commissario del governo per l'attuazione dell'Agenda digitale. L'ANPR è costituita dall'Indice nazionale delle anagrafi e dall'Anagrafe degli italiani residenti all'estero, ed è destinata a subentrare alle preesistenti anagrafi comunali. La nuova base dati di interesse nazionale sarà accessibile alle pubbliche amministrazioni e agli organismi che erogano servizi pubblici. L'Anagrafe nazionale metterà tra l'altro a loro disposizione l'indirizzo di posta elettronica certificata indicato dal cittadino come proprio domicilio digitale e assicurerà il servizio di invio telematico delle attestazioni, delle dichiarazioni di nascita e dei certificati di morte[24].

2. I pagamenti elettronici nell'Agenda digitale

2.1 La diffusione dei pagamenti elettronici

I pagamenti elettronici sono una parte fondamentale dell'economia digitale. Il commercio elettronico, in particolare, è ampiamente basato sui pagamenti elettronici a distanza. Il settore ha importanti prospettive di crescita. Per comprendere le dimensioni del fenomeno, è utile fare riferimento ad alcuni dati recenti.

Nell'Unione europea, secondo gli ultimi dati della Banca Centrale Europea[25], il numero dei pagamenti **con strumenti diversi dal contante** ha raggiunto nel 2012 94,5 miliardi, con un aumento del 4,2% rispetto all'anno precedente. I pagamenti con carte (di debito e di credito) rappresentano il 42% del totale delle transazioni, i bonifici il 27%, gli addebiti diretti il 24%, la moneta elettronica e gli altri strumenti di pagamento il 2,1% (v. Figura 1 in Allegato).

In particolare, il numero delle carte di pagamento ha raggiunto 738 milioni (che corrispondono a 1,46 carte per abitante). Il numero delle transazioni con carta è cresciuto del 7,3%, raggiungendo 39,8 miliardi di operazioni, per un totale di 2000 miliardi di euro. A ciò corrisponde un valore medio di 51 euro per operazione.

Per quanto riguarda i punti di accesso al sistema dei pagamenti nell'Unione europea, nel 2012 il numero degli ATM è diminuito dello 0,4% rispetto all'anno precedente (440.000 dispositivi), mentre il numero dei POS è aumentato del 7,9%, raggiungendo 9,7 milioni.

[24] Articolo 2 del decreto legge n. 179/2012, convertito dalla legge n. 221/2012; cfr. anche il decreto del Presidente del Consiglio dei Ministri 23 agosto 2013, n. 109, recante le misure di prima attuazione dell'ANPR.
[25] European Central Bank, Payment statistics for 2012, 10 settembre 2013.

L'utilizzo dei diversi strumenti varia significativamente tra gli Stati membri. Sempre secondo i dati BCE, nel 2012 in Italia il 39% delle transazioni è stato realizzato con carta, il 29,11% con bonifico, il 13,9% con addebito diretto (Figura 2 in Allegato).

Data la diffusione di modelli sociali e commerciali che richiedono pagamenti in ogni momento, con qualsiasi strumento e in qualunque luogo, gli attori che offrono servizi di pagamento sono sempre più numerosi (banche, imprese di telecomunicazione, utilities, imprese della distribuzione commerciale, *travel and transportation).* La domanda da parte dei consumatori e la concorrenza tra gli operatori contribuiscono ad accelerare il processo di sostituzione del contante con strumenti di pagamento più efficienti.

I **servizi di pagamento via internet** (che possono essere basati su carte di pagamento, bonifici, addebiti diretti o strumenti prepagati gestiti da prestatori di servizi di pagamento) avranno un ruolo crescente con lo sviluppo del commercio elettronico. Va tenuto presente, a questo riguardo, che gli acquisti on-line oggi rappresentano solo il 3,4% delle vendite al dettaglio nell'Unione europea[26], ma secondo le stime di Forrester Research nei prossimi cinque anni dovrebbero aumentare a un tasso annuo del 10%[27].

Il metodo di pagamento con le maggiori prospettive di crescita a livello mondiale è costituito dai pagamenti con dispositivo mobile (***m-payments*****)**, effettuati utilizzando il cellulare o il tablet. Questi pagamenti, utilizzabili sia per gli acquisti on-line che per quelli di prossimità, possono essere collegati a un conto bancario (pagamenti su carta, bonifici o addebiti diretti), essere realizzati con carte pre-pagate o conti dedicati non connessi a un conto bancario (moneta elettronica) oppure anche mediante l'addebito diretto al consumatore sul credito telefonico o sul conto telefonico. La diffusione dei dispositivi mobili e la possibilità di utilizzarli per piccoli pagamenti può aiutare a diffondere tra la popolazione l'abitudine al pagamento con denaro elettronico.

La diffusione dei pagamenti con dispositivo mobile in Europa è ancora relativamente modesta rispetto ad altre aree geografiche: nel 2012 gli utilizzatori di *m-payments* erano 85 milioni in Asia, 57,8 milioni in Africa, 32,8 milioni in NordAmerica e solo 26,7 milioni in Europa. Le stime di crescita del valore degli *m-payments* a livello mondiale considerate dalla Commissione europea indicano tassi di sviluppo in una range tra il 37% e il 100% all'anno nel prossimo triennio.

---

[26] Commission Staff Working Document, *Online services, including e-commerce, in the Single Market*, SEC(2011) 1641.

[27] Cfr. Commission Staff Working Document, *Impact assessment accompanying the proposal for a directive on payment servies in the internal market and the proposal for a regulation on interchange fees for card-based payment transactions*, SWD(2013) 288 final; cfr. Anche http://www.forrester .com/European+Online+Retail+Forecast+2010+To+2015/fulltext/-/E-RES58597.

In Italia, secondo i dati 2012 dell'Osservatorio NFC & Mobile Payment del Politecnico di Milano[28], in un anno il valore delle transazioni in remoto effettuate attraverso dispositivo mobile (*Mobile Remote Payment and Commerce)* è aumentato del 30%, passando da 700 milioni a 900 milioni di euro. Più della metà riguarda l'acquisto di contenuti digitali per smartphone (470 milioni di euro, +15% rispetto al 2011), ma l'acquisto di altri beni e servizi ha registrato un forte aumento (310 milioni di euro, + 60% rispetto al 2011). I trasferimenti di denaro tramite dispositivo mobile (Mobile Money Transfer) hanno raggiunto il valore di 150 milioni di euro (+50% rispetto al 2011) (Figura 3 in Allegato).

In futuro, è prevista in particolare una rapida crescita dei pagamenti tramite dispositivo mobile per le spese relative alla mobilità, in stretta connessione con esigenze di pubblica utilità (parcheggi, biglietti degli autobus, ricariche degli abbonamenti per il trasporto pubblico locale, taxi). Secondo le stime del Politecnico di Milano, nel 2012 sono stati oltre 700.000 i pagamenti tramite dispositivo mobile di ore di parcheggio, oltre 600.000 i biglietti di corsa semplice acquistati, qualche migliaio le ricariche di abbonamenti per il trasporto pubblico locale attivate e quasi 10.000 i pagamenti di corse di taxi[29]. Gli sviluppi nei primi mesi del 2013 indicano una forte ulteriore accelerazione, anche a seguito delle misure normative a favorire la diffusione del servizio (sul tema, cfr. il successivo paragrafo 3.3)[30].

I terminali POS con tecnologia *Near Field Communication* (NFC) che consentono il pagamento di prossimità mediante dispositivo mobile nel 2012 erano circa 30.000 (5.000 nel 2011), e si prevede che nel 2013 possano superare le 170.000 unità. Un recente sviluppo che può contribuire alla diffusione dei pagamenti elettronici anche presso piccoli commercianti è costituito da dispositivi molto piccoli che si collegano direttamente allo smartphone o al tablet dell'operatore trasformandolo in un vero e proprio POS (c.d. mobile POS).

I cellulari dotati di tecnologia NFC venduti nel 2012 sono stati 2,5 milioni e le stime per il 2013 raggiungono i 6 milioni.

Un'ulteriore diffusione dei pagamenti elettronici costituisce per più ragioni un importante obiettivo per la politica pubblica: ne può derivare una significativa riduzione dei costi di gestione del sistema, una maggiore velocità dei pagamenti e la semplificazione delle modalità di pagamento per i consumatori, anche per transazioni di piccole dimensioni, con un possibile effetto positivo sul volume complessivo degli acquisti. Inoltre i pagamenti elettronici, a differenza

[28] Osservatorio NFC&Mobile Payment, *Mobile Payment: l'Italia s'è desta!*, febbraio 2013.

[29] La sperimentazione condotta a Firenze per il pagamento dei biglietti del trasporto pubblico locale mediante dispositivo mobile ha portato significativi risultati, con una media di 140.000 biglietti venduti ogni mese (dati aprile 2012).

[30] A Genova, a due mesi dal lancio del servizio di pagamento dei biglietti del trasporto pubblico locale mediante dispositivo mobile, si registravano già 12.000 clienti (dati luglio 2013).

dell'uso del contante, consentono la tracciabilità delle operazioni e sono funzionali al contrasto all'evasione fiscale.

Proposizione 20 – Una maggiore diffusione dei pagamenti elettronici nelle varie modalità può ridurre i costi di gestione per gli operatori, assicurare la velocità dei pagamenti e semplificare l'acquisto dei beni e servizi da parte dei consumatori; indirettamente, essa può anche contribuire alla tracciabilità delle operazioni e al contrasto dell'evasione fiscale.

2.2 Le iniziative europee

Nella prospettiva europea, assicurare che la disponibilità per le imprese e i consumatori di servizi di pagamento elettronico "sicuri, efficienti, concorrenziali e innovativi" utilizzabili, senza ostacoli transfrontalieri, in tutto il territorio dell'Unione europea è funzionale alla piena realizzazione del Mercato unico. Inoltre la qualità dei pagamenti elettronici è un fattore determinante per lo sviluppo del commercio elettronico in Europa e quindi per la realizzazione dell'Agenda digitale europea.

I vantaggi economici di una maggiore integrazione del mercato dei pagamenti in Europa sono rilevanti. Ad esempio, il progetto di realizzazione di uno spazio integrato dei pagamenti in euro (SEPA) per i bonifici, gli addebiti diretti e le carte di pagamento può produrre a regime benefici diretti e indiretti per più di 360 miliardi di euro su un periodo di sei anni[31].

Le iniziative legislative europee in tema di pagamenti al dettaglio hanno avvio con il regolamento (CE) n. 2560/2001 sui pagamenti transfrontalieri in euro, poi sostituito dal regolamento (CE) n. 924/2009. In particolare, con questi regolamenti sono state eliminate le differenze nelle commissioni applicate agli utilizzatori di servizi di pagamento per i pagamenti transfrontalieri rispetto ai pagamenti nazionali in euro. La disciplina si applica a tutti i pagamenti che comportano l'utilizzo di un processo elettronico (inclusi bonifici, addebiti diretti, prelievi di contante dagli ATM, pagamenti con carte di debito e di credito).

Con il regolamento (CE) n. 1781/2006 sono state introdotte regole europee per prestatori di servizi di pagamento sui dati informativi relativi all'ordinante che accompagnano i trasferimenti di fondi, al fine di prevenire, investigare e individuare casi di riciclaggio di denaro e finanziamento del terrorismo[32].

[31] *SEPA: potential benefits at stake*, CapGemini, 2007.

[32] Con la direttiva 2005/60/CE del 26 ottobre 2005 erano state adottate disposizioni per la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e finanziamento del terrorismo; la direttiva 2006/70/CE del 1° agosto 2006 reca le misure di esecuzione.

Nel 2007 è stata adottata la direttiva sui servizi di pagamento nel mercato interno, che fissa una serie di regole comuni per rimuovere gli ostacoli alla creazione di un mercato europeo integrato, facilitare la realizzazione concreta del SEPA e favorire l'entrata di nuovi operatori (gli istituti di pagamento). La direttiva stabilisce in particolare regole armonizzate sui requisiti informativi, i diritti e gli obblighi connessi alla prestazione dei servizi di pagamento[33].

Con la direttiva 2009/110/CE[34] sono state invece fissate regole comuni per l'avvio e l'esercizio dell'attività di emissione di moneta elettronica (strumenti di pagamento pre-pagati), allineando i requisiti di vigilanza prudenziale a quelli già previsti per i prestatori di servizi di pagamento dalla direttiva 2007/64/CE.

Il regolamento (CE) n. 260/2012 ha fissato al 1° febbraio 2014 il termine per la migrazione al SEPA per i bonifici e gli addebiti diretti in euro. La disciplina, che ha apportato alcune modifiche al regolamento (CE) 924/2009, include disposizioni sulle commissioni interbancarie per le operazioni di addebito diretto[35].

Nel 2011 la Commissione ha avviato un'ampia consultazione pubblica sulle ulteriori misure che potrebbero favorire la realizzazione di un mercato europeo integrato per i pagamenti attraverso carte, internet e dispositivi mobili[36]. La premessa è che le modalità con cui i consumatori effettuano i propri acquisti stanno cambiando significativamente e che lo sviluppo di pagamenti elettronici innovativi integrati a livello europeo è un fattore fondamentale di traino per il mercato unico digitale e lo sviluppo del commercio elettronico, e può fornire un forte impulso alla crescita e alla competitività dell'economia europea. La Commissione si sofferma, in particolare, sulle seguenti esigenze: ridurre la frammentazione dei mercati e gli ostacoli all'entrata, anche a livello transfrontaliero; aumentare la trasparenza e la connessione ai costi dei prezzi dei servizi di pagamento per consumatori, dettaglianti e altre imprese; rafforzare la standardizzazione a livello europeo, in modo da favorire l'interoperabilità tra i servizi; rafforzare la sicurezza dei pagamenti.

---

[33] Direttiva 2007/64/CE del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE.

[34] Direttiva 2009/110/CE del 16 settembre 2009 concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE.

[35] Regolamento (UE) n. 260/2012 del Parlamento europeo e del Consiglio del 14 marzo 2012 che stabilisce i requisiti tecnici e commerciali per i bonifici e gli addebiti diretti in euro e che modifica il regolamento (CE) n. 924/2009 .

[36] Commissione europea, Green Paper *"Towards an integrated European Market for card, internet and mobile payments*, COM(2011) 941 def.

Il 24 luglio 2013 la Commissione ha presentato un pacchetto di misure legislative in tema di pagamenti, composto da una proposta di direttiva sui servizi di pagamento nel mercato interno, destinata a sostituire la direttiva del 2007[37] e da una proposta di regolamento sulle commissioni interbancarie per le transazioni basate su carte di pagamento[38].

Soffermandoci in questa sede solo sulla proposta di direttiva, la Commissione prende atto dello sviluppo di nuovi servizi che possono svolgere un ruolo importante nel soddisfare le esigenze dei consumatori e dei venditori, tra cui in particolare i *payment initiation services,* con cui l'utente di internet viene collegato rapidamente alla piattaforma di online banking della banca di cui è cliente, così da potere effettuare il pagamento via internet (tipicamente tramite bonifico), senza necessità di utilizzare una carta[39], e i servizi di informazione sul conto (*account information services*), che forniscono all'utilizzatore di servizi di pagamento informazioni in forma facilmente utilizzabile sulle disponibilità presenti sul conto detenuto dal soggetto presso un prestatore di servizi di pagamento.

Per favorire la concorrenza nella prestazione di servizi di pagamento ed evitare, al tempo stesso, conseguenze indesiderabili in termini di sicurezza e protezione dei dati personali, la Commissione si propone di modificare la precedente disciplina in modo da creare un *level playing field* tra gli operatori. Come sottolineato dal Commissario Barnier, "*il ne devrait y avoir aucun obstacle injustifié à l'accès au marché des nouveaux prestataires, dès lors que la sécurité des paiements est garantie*"[40]. In particolare, per consentire ai nuovi prestatori di servizi di pagamento l'accesso alle informazioni sulla disponibilità finanziaria nel conto di un soggetto occorre prima definire un rigoroso sistema volto a evitare i rischi che potrebbero derivare dall'accesso a questa informazione.

Coerentemente con questa prospettiva, la proposta di direttiva introduce una serie di requisiti che devono essere soddisfatti dai *third-party payment service providers* – TPPs, ossia dai

[37] Cfr. 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 and 2009/110/CE e che abroga la direttiva 2007/64/CE, 2013/0264(COD).

[38] Proposta di regolamento del Parlamento europeo e del Consiglio relativo alle commissioni interbancarie sulle operazioni di pagamento tramite carta, 2013/0265(COD). In particolare, la proposta di regolamento prevede che per tutte le carte di pagamento utilizzate dai consumatori ("must take") sia posto un tetto alle commissioni interbancarie (0,2% per le carte di debito e 0,3% per le carte di credito), inizialmente solo per le transazioni cross border e in seguito anche all'interno degli Stati membri e che sia consentito ai dettaglianti acquistare i servizi da banche stabilite in altri Stati membri.

[39] Come avviene attraverso il sistema MyBank, basato su un'infrastruttura paneuropea gestita da EBAClearing che consente l'accesso dal sito web dell'esercente al proprio conto bancario online per effettuare il pagamento.

[40] Cfr. Michel Barnier, *Pour un vrai marché unique des paiements par carte, internet et mobile*, speech/12/329 presentato alla Conferenza *Card, internet and mobile payments*, organizzata dalla Commissione europea il 4 maggio 2012.

prestatori dei nuovi servizi diversi dalle banche presso le quali il soggetto che effettua il pagamento detiene un conto. La proposta prevede in particolare che i TPPs debbano essere registrati e sottoposti alla vigilanza prevista per gli istituti di pagamento e siano assoggettati agli stessi diritti e obblighi degli altri prestatori di servizi di pagamento. Sono fissati specifici requisiti in tema di sicurezza e di protezione dei dati personali. I prestatori che rispettano quanto previsto dalla direttiva avranno il diritto di ottenere dalla banca, non appena ricevono l'ordine di pagamento, informazioni sulla disponibilità di fondi sul conto del soggetto.

Proposizione 21 – L'obiettivo di creare un effettivo *level playing field* tra gli operatori, perseguito dalla proposta di direttiva sui servizi di pagamento, è condivisibile. Nel settore dei pagamenti l'esigenza di favorire lo sviluppo di nuovi servizi in un contesto concorrenziale va contemperata con quella, imprescindibile, di garantire la sicurezza e la tutela dei dati personali.

Al di là delle specifiche previsioni contenute nella proposta di direttiva, nel settore dei pagamenti elettronici, così come in quello dell'identificazione elettronica, la standardizzazione svolge un ruolo essenziale per assicurare l'interoperabilità delle soluzioni, sia a livello europeo che a livello internazionale. Occorre continuare a lavorare su questo fronte per garantire l'interoperabilità anche rispetto allo sviluppo di nuovi servizi.

Proposizione 22 – Alla standardizzazione spetta il compito di assicurare l'interoperabilità delle soluzioni nel settore dei pagamenti, anche in relazione allo sviluppo dei nuovi servizi: si tratta quindi di un ruolo cruciale per lo sviluppo del mercato.

Per quanto attiene alla sicurezza, dalle indagini svolte per conto della Commissione europea sulle cause del mancato utilizzo del commercio elettronico emerge che i consumatori sono soprattutto frenati da timori di frodi. Per favorire l'utilizzo degli strumenti di pagamento in remoto e quindi indirettamente anche il ricorso al commercio elettronico, occorre da un lato continuare la ricerca di soluzioni sicure[41] e garantire un'efficiente azione di contrasto alle frodi[42], dall'altro svolgere un'attività di informazione dei consumatori circa gli strumenti a loro disposizione per tutelarsi, in modo da aumentarne la fiducia.

[41] Richiedere un'autenticazione basata su due elementi in genere è considerata una buona pratica. Un punto di riferimento essenziale in materia di sicurezza sono i lavori svolti nell'ambito del SecuRe Pay Forum. Cfr. in particolare i recenti rapporti "Recommendations for the Security of Internet Payments" e "Recommendations for Payment Account Access Services", entrambi disponibili sul sito della BCE.

[42] Cfr., tra l'altro, la proposta di direttiva del Parlamento europeo e del Consiglio recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione, COM(2013) 48 def. e il regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio del 21 maggio 2013 relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), che abroga il regolamento (CE) n. 460/2004.

Proposizione 23 – L'utilizzo dei pagamenti in remoto dipende dalla fiducia dei soggetti sulla loro affidabilità e sull'esistenza di sistemi idonei a arginare il rischio di frodi. Oltre a investire nella ricerca di soluzioni sicure e a garantire un'efficace azione di contrasto alle frodi, è essenziale informare il consumatore degli strumenti a disposizione per arginare i rischi, così da indurlo a avvicinarsi con fiducia alle nuove soluzioni. Un ruolo centrale può essere svolto in questo contesto dai *trustmarks* che indicano in modo facilmente riconoscibile per il consumatore che il sistema di pagamento offerto da un sito soddisfa elevati requisiti di sicurezza.

2.3 Le iniziative in Italia

In Italia, oltre al recepimento delle norme europee relative ai servizi di pagamento[43], nell'ultimo biennio sono state adottate alcune disposizioni volte a favorire la diffusione dei pagamenti elettronici, con il decreto legge 6 dicembre 2011, n. 201 (cosiddetto "Salvaitalia"), convertito con modificazioni dalla legge 22 dicembre 2011, n. 214 e con il decreto legge 18 ottobre 2012, n. 179 (cosiddetto "Sviluppo bis"), convertito con modificazioni dalla legge 17 dicembre 2012, n. 221. Queste disposizioni mirano in particolare a incentivare il ricorso di questi strumenti prevedendone l'utilizzo nei rapporti con la pubblica amministrazione.

a) Pagamenti alle pubbliche amministrazioni mediante tecnologie ICT

In base all'articolo 5 del Codice dell'amministrazione digitale (CAD)[44] tutte le pubbliche amministrazioni (anche locali) **devono consentire sul territorio nazionale l'effettuazione dei pagamenti ad esse spettanti, a qualsiasi titolo dovuti, con l'uso delle tecnologie dell'informazione e della comunicazione**. Sono fatte salve le attività di riscossione dei tributi, regolate da normative specifiche. A tal fine, le pubbliche amministrazioni devono indicare sui propri siti istituzionali e sulle richieste di pagamento i codici identificativi .del conto .tramite il quale i soggetti possono effettuare i pagamenti mediante bonifico bancario o postale o mediante bollettino postale, nonché i dati e i codici da indicare nella causale di versamento. Le pubbliche amministrazioni centrali possono avvalersi, "senza nuovi o maggiori oneri per la finanza pubblica", di prestatori di servizi di pagamento per consentire ai privati di effettuare i pagamenti in loro favore attraverso strumenti elettronici. Il prestatore di servizi di pagamento che riceve l'importo lo riversa al tesoriere dell'ente e registra in un apposito sistema informatico

[43] Decreto legislativo 27 gennaio 2010, n. 11, di attuazione della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno; decreto legislativo 16 aprile 2012, n. 45, di attuazione della direttiva 2009/110/CE concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica.
[44] Decreto legislativo 7 marzo 2005, n. 82.

a disposizione dell'amministrazione il pagamento eseguito, la relativa causale e gli altri dati rilevanti.

Le regole tecniche per l'attuazione dell'articolo 5, attese da anni, non sono ancora state adottate. Recentemente ne è stata pubblicata una bozza sul sito dell'Agenzia per l'Italia digitale, sottoponendola a consultazione pubblica ("Linee guida per l'effettuazione dei pagamenti elettronici a favore delle pubbliche amministrazioni e dei gestori di pubblici servizi", ex articolo 5, comma 4, del CAD)[45].

Il decreto legge n. 201/2011 ha previsto la stipulazione di convenzioni con gli intermediari finanziari per fornire alle amministrazioni pubbliche POS a condizioni agevolate al fine di consentire la riscossione dei pagamenti da parte del pubblico con strumenti diversi dal contante.

Con il decreto legge n. 179/2012 la disciplina che obbliga le pubbliche amministrazioni ad accettare i pagamenti anche con tecnologie ICT è stata resa più dettagliata, fissando regole uniformi per tutti i livelli di amministrazione, centrali e locali, e prevedendo l'assimilazione alla PA dei gestori di pubblici servizi, limitatamente ai rapporti con l'utenza. È inoltre prescritto che i prestatori di servizi di pagamento dovranno essere scelti dalle amministrazioni mediante ricorso agli strumenti di acquisto e negoziazione messi a disposizione dalla Consip. È previsto inoltre che con decreto ministeriale sia disciplinata l'estensione delle modalità di pagamento includendo anche le tecnologie mobili.

b) Pagamenti delle pubbliche amministrazioni tramite tecnologie ICT

L'articolo 12 del decreto legge n. 201/2011 ha sancito l'**obbligo per le pubbliche amministrazioni centrali e locali** e per i loro enti di effettuare i pagamenti delle spese mediante l'utilizzo di strumenti telematici. Anche i pagamenti da parte delle pubbliche amministrazioni degli stipendi, delle pensioni e dei compensi superiori a 500 euro non possono essere effettuati tramite contante.

c) Altre disposizioni del decreto Salvaitalia

Oltre a quanto già indicato, il decreto legge n. 201/2011:

- ha sancito il divieto di utilizzo del contante per transazioni superiori a 999 euro;
- ha introdotto il conto corrente di base, senza spese, per le fasce svantaggiate della popolazione, interamente a carico degli operatori del settore. Sarebbe stato forse più

[45] Cfr. http://www.digitpa.gov.it/sites/default/files/notizie/LineeGuidaPagamenti_V_1_0_1.pdf.

corretto concepire il servizio come un servizio di interesse economico generale, accompagnato da compensazioni per i connessi obblighi di servizio pubblico. Una tale impostazione, che potrebbe essere realizzata con l'attribuzione di voucher agli aventi diritto, avrebbe probabilmente contribuito a una maggiore promozione e diffusione del nuovo servizio[46];

- con l'obiettivo di promuovere la diffusione delle carte di pagamento aveva previsto un sistema piuttosto dirigistico e potenzialmente in contrasto con il diritto europeo di tetto massimo (pari all'1,5 per cento) per le commissioni a carico degli esercenti commerciali sui pagamenti effettuati con carta (c.d. *merchant fees*). La disposizione è stata successivamente eliminata. Il compito di definire le regole generali per assicurare il contenimento delle commissioni è stato affidato a un tavolo tra operatori, mentre spetta alle pubbliche autorità la valutazione dell'efficacia delle misure proposte e la loro eventuale conferma con decreto.

d) Altre disposizioni del decreto "Sviluppo bis"

Le altre disposizioni del decreto legge n. 179/2012 in materia di pagamenti, oltre a quelle già citate, prevedono:

- l'obbligo a partire dal 1° gennaio 2014 per i soggetti che effettuano attività di vendita di prodotti e di prestazione di servizi, inclusi i servizi professionali, **di accettare** anche i **pagamenti mediante carte di debito**. Saranno fissati con decreti interministeriali eventuali importi minimi, modalità e termini e si potrà estendere l'obbligo di accettazione ad altri strumenti di pagamento, anche **con tecnologie mobili**;
- l'obbligo per le aziende di trasporto pubblico locale di promuovere l'adozione di sistemi di **bigliettazione elettronica interoperabili** a livello nazionale. Le regole tecniche devono essere adottate con decreto ministeriale. Dovrà essere consentito l'utilizzo della bigliettazione elettronica attraverso **strumenti di pagamento in mobilità**, anche tramite qualsiasi dispositivo di telecomunicazione.

L'efficacia della maggior parte di queste misure dipende dall'adozione di successivi provvedimenti attuativi.

Proposizione 24 – Le disposizioni legislative volte a promuovere la diffusione dei pagamenti con tecnologie ICT, in particolare nei rapporti con le pubbliche amministrazioni, potranno produrre risultati solo quando saranno adottate le previste

[46] Sul tema, cfr. Vincenzo Meli, *Il conto corrente di base tra inclusione finanziaria e controllo della circolazione della ricchezza*, in corso di pubblicazione su "Banca, borsa e titoli di credito".

misure attuative. Il completamento della disciplina dovrebbe essere visto come una priorità nell'ambito dell'Agenda digitale italiana.

Disposizioni attuative in tema di fatture elettroniche

Dopo l'adozione della legge 24 dicembre 2012, n. 228 sulle fatture elettroniche di recepimento della direttiva 2010/45/UE, si apre una nuova fase di definizione degli standard volti a consentire l'interoperabilità delle soluzioni. È in via di elaborazione a livello europeo una direttiva che richiede la fatturazione elettronica per tutti gli appalti pubblici[47], in analogia con le regole esistenti da tempo nel nostro ordinamento sull'obbligo di fatturazione elettronica nei rapporti con la pubblica amministrazione, che nel maggio 2013 sono state completate con la disciplina attuativa[48].

Secondo i dati più recenti dell'Osservatorio "Fatturazione elettronica e Dematerializzazione" del Politecnico di Milano, dall'obbligo di utilizzo della fatturazione elettronica nei confronti delle pubbliche amministrazioni si possono ottenere risparmi superiori ad un miliardo di euro l'anno per le pubbliche amministrazioni e di circa 1,6 miliardi di euro per le imprese.

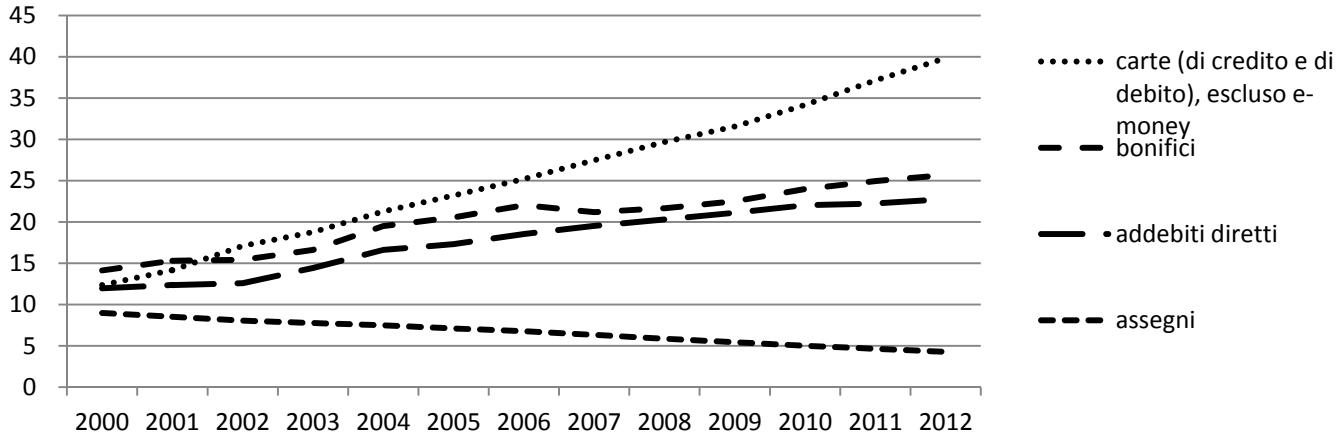
Inoltre, se la fatturazione elettronica venisse utilizzata anche solo nel 20 per cento dei rapporti tra le imprese si potrebbero risparmiare ulteriori tre miliardi di euro l'anno. Infine, se si giungesse alla digitalizzazione dell'intero ciclo dell'ordine sia nei rapporti con le pubbliche amministrazioni che nei rapporti tra imprese, i risparmi raggiungerebbero 60 miliardi.

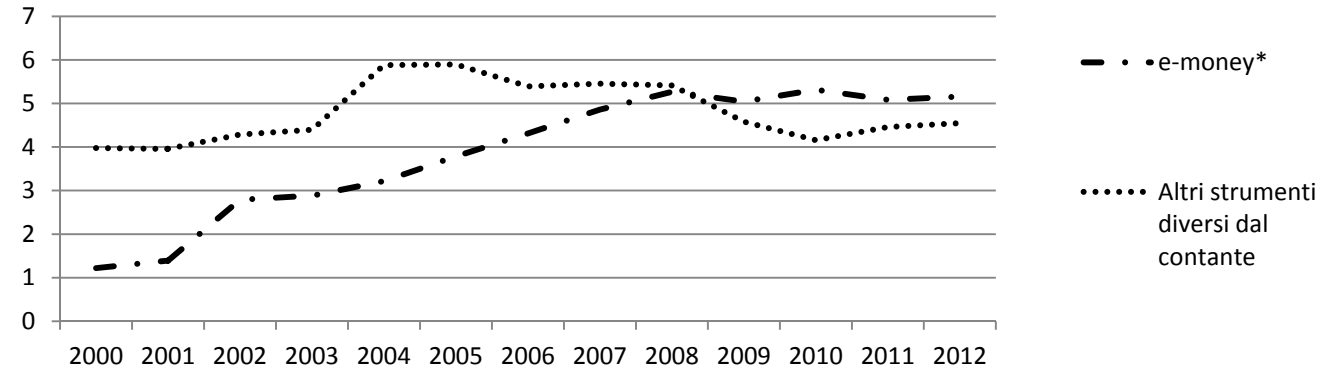
Proposizione 25 – I benefici derivanti da un efficiente sistema di pagamenti elettronici sarebbero potenziati se in parallelo si diffondesse effettivamente il ricorso alla fatturazione elettronica negli Stati membri. I vantaggi stimati, nel caso di digitalizzazione dell'intero ciclo dell'ordine, raggiungono 60 miliardi di euro.

[47] COM(2013) 449 def.
[48] Decreto ministeriale n. 55 del 3 aprile 2013, emanato ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244.

FIGURA 1

Stima del numero di transazioni per tipo di strumento di pagamento nell'Unione europea (2000 – 2012) (in miliardi)



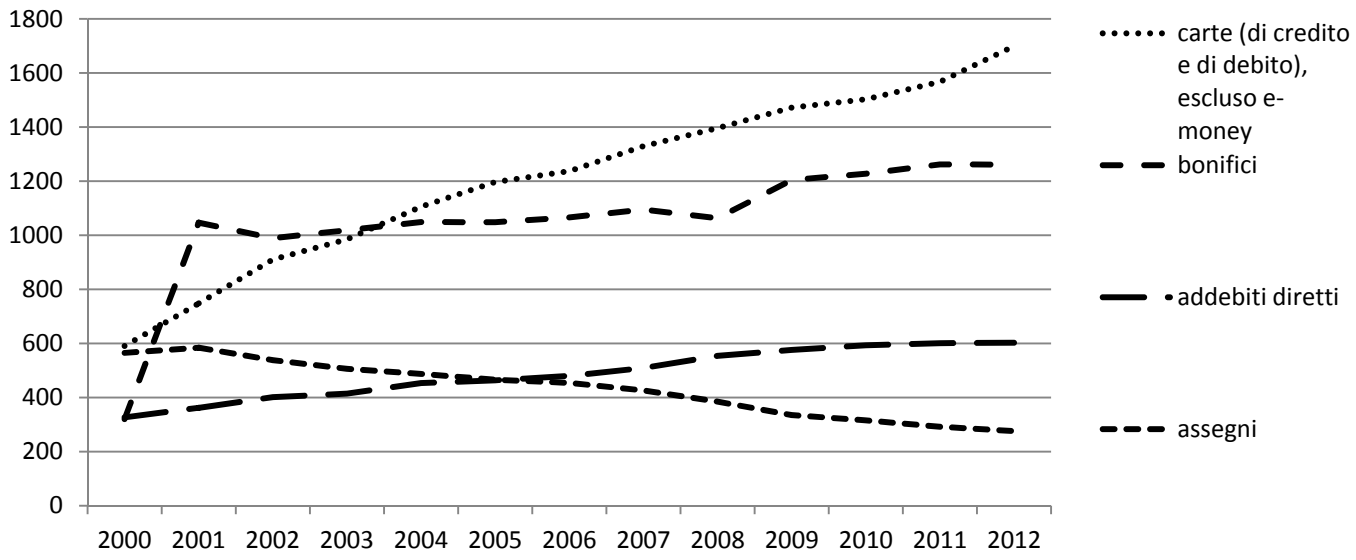


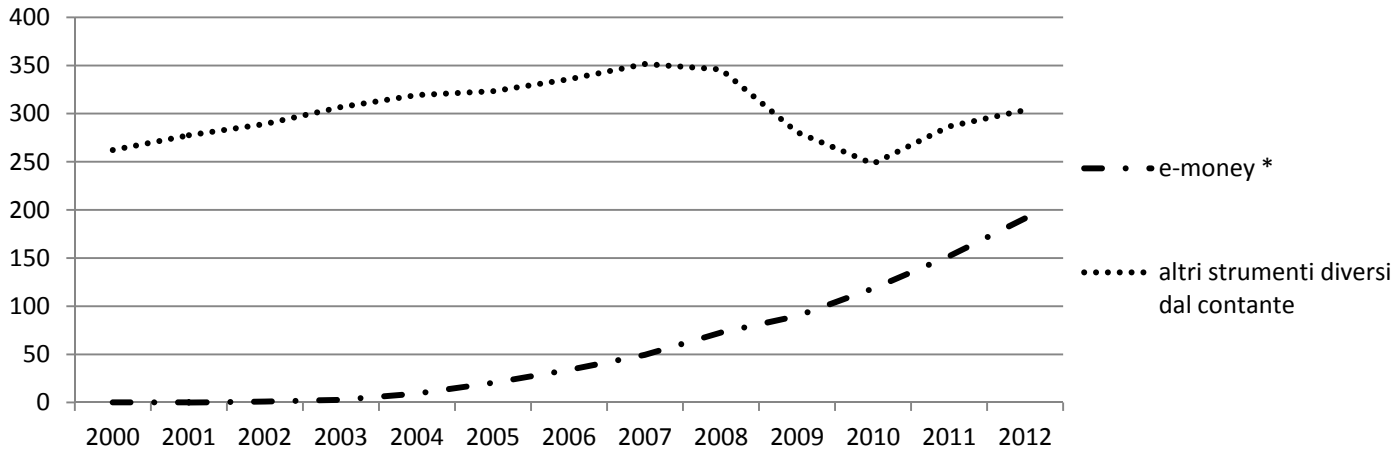
Fonte: Banca Centrale Europea, *Payment statistics*, dati aggiornati a settembre 2013

* Per e-money (moneta elettronica) si intendono i pagamenti effettuati mediante strumenti prepagati.

FIGURA 2

Stima del numero di transazioni per tipo di strumento di pagamento in Italia (2000 – 2012) (in milioni)





Fonte: Banca Centrale Europea, *Payment statistics*, dati aggiornati a settembre 2013

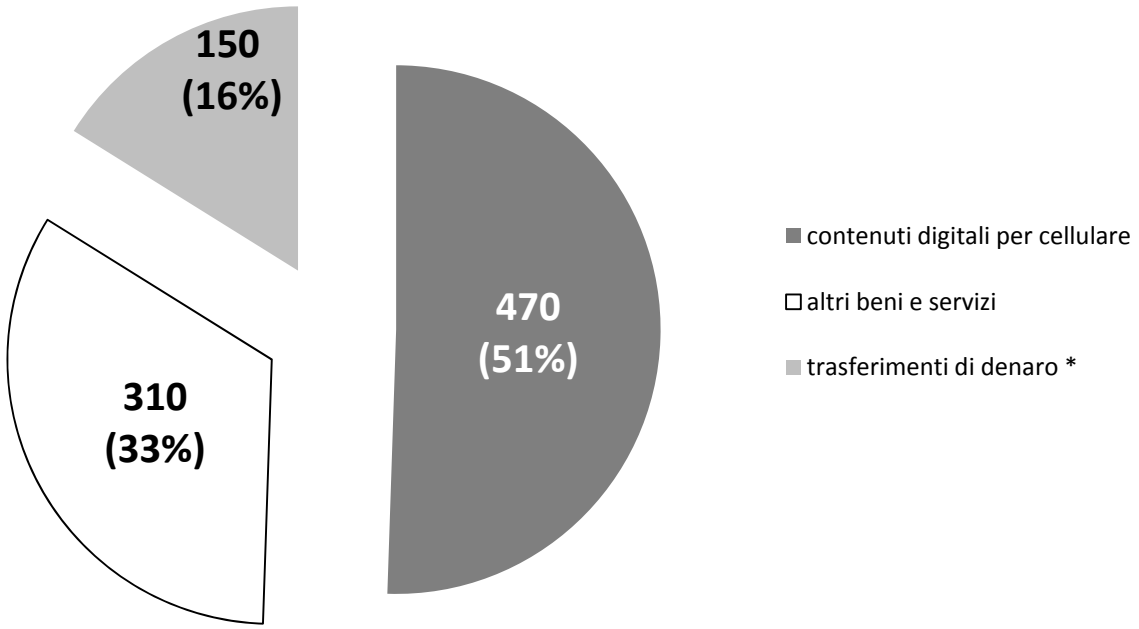
n.b. Per gli anni 2000-2001, non si hanno dati rispetto all'utilizzo di e-money in Italia.

* Per e-money (moneta elettronica) si intendono i pagamenti effettuati mediante strumenti prepagati.

FIGURA 3

Composizione del Mobile Remote Payment & Commerce in Italia per tipologia di acquisto (2012)

(in milioni di euro)



Fonte: Osservatorio NFC & Mobile Payment, Rapporto 2013

* tra i trasferimenti di denaro (Mobile Money Transfer) vanno inclusi le ricariche di carte prepagate, i trasferimenti di credito telefonico e i trasferimenti di somme tra persone