

La *digital economy* e la condivisione dei dati per finalità di *business*: ostacoli ed opportunità

A cura di:

CRIF S.p.A.
via Mario Fantin 1/3
40131 Bologna BO

Contatto:

Luisa Monti
e-mail: l.monti@crif.com
telefono: 051 417 6111

Contents

Introduzione	3
Il <i>framework</i> regolamentare e normativo europeo.....	5
EDPS, Article 29 WP e la nuova General Data Protection Regulation	6
Il complesso normativo-regolamentare: una selva oscura	8
Bitcoin, blockchain e DLT.....	9
Digital Single Market Strategy	11
Identificazione elettronica.....	12
E in Italia?	14
Wrap up	17
Appendice: Posizione Italiana sul mercato unico digitale	20

Introduzione

L'economia europea si trova ormai da tempo in una situazione di crescita bassissima, caratterizzata da una dinamica dei prezzi preoccupante (con Paesi a rischio deflazione) e da tassi di disoccupazione elevati. Il persistere di bassi livelli di crescita della produttività continua a perpetuare squilibri a livello macroeconomico. La concorrenza delle economie emergenti in vari settori industriali, manifatturieri e agricoli non è destinata ad allentare la pressione.

Come si evince dal documento di lavoro della Commissione europea, recante la relazione relativa all'Italia per l'anno 2015¹, il nostro Paese sconta ulteriori scostamenti rispetto all'Unione europea e all'eurozona a causa dell'elevato livello del debito pubblico e della debolezza della competitività esterna. Il PIL reale italiano è sceso ai livelli dei primi anni 2000, mentre il PIL della zona euro è superiore a quei livelli di oltre il 10%.

Nonostante alcune significative riforme, l'Italia non ha ancora registrato miglioramenti altrettanto significativi: la debole crescita della produttività continua a spingere al rialzo il costo del lavoro per unità di prodotto, mentre i fattori non di costo restano sfavorevoli. La competitività dell'Italia sul mercato delle esportazioni resta debole. Inoltre l'elevata percentuale di piccole imprese con una posizione competitiva debole sui mercati internazionali ostacola ulteriormente la competitività internazionale del nostro Paese.

Infine va sottolineata la drastica riduzione del livello di investimenti causata dalla grave crisi economica, nonché il deterioramento a lungo termine della loro qualità. Gli investimenti produttivi in Italia sono infatti diminuiti in misura significativa, e sono ora inferiori dell'1,5% alla media dell'UE in percentuale del PIL.

Le barriere concorrenziali sui mercati dei prodotti/servizi, le carenze infrastrutturali e i bassi livelli di spesa per ricerca e sviluppo, in particolare da parte delle imprese, rappresentano un notevole ostacolo la crescita della produttività. Sebbene nell'aprile 2015 il Governo italiano abbia presentato un disegno di legge sulla concorrenza², tuttora in

¹ Commissione europea, Brussels, 18.3.2015, SWD (2015) 31 Final/2, Documento di lavoro dei servizi della Commissione. Relazione per paese relativa all'Italia 2015 comprensiva dell'esame approfondito sulla prevenzione e la correzione degli equilibri macroeconomici.

² Disegno di legge C. 3012, presentato il 3 aprile 2015 alla Camera dei Deputati e trasmesso al Senato l'8 ottobre 2015 (Disegno di legge S. 2085).

itinerare, che mira a rimuovere gli ostacoli alla concorrenza in diversi settori dell'economia, le misure previste possono essere considerate di incisività e portata variabili.

In questo scenario la rivoluzione dell'economia digitale rappresenta un'occasione che l'Italia e l'Europa tutta non possono assolutamente permettersi di trascurare, pena l'exasperato ed irreversibile ampliamento del divario competitivo tra le imprese italiane e quelle oltreoceano e lo svantaggio dei cittadini nell'ottenimento dei benefici derivanti dalla agevole fruizione di servizi innovativi. L'Italia sconta già in termini di PIL lo scarso investimento livello di investimento nella digitalizzazione.

Il successo della rivoluzione digitale passa per la consapevolezza che il dato ha un proprio valore intrinseco e intersettoriale accresciuto dalla possibilità di diffonderlo in maniera capillare e su larga scala e dalle enormi capacità di elaborazione offerta dalle moderne tecnologie.

A livello italiano ed europeo si rileva un approccio regolamentare eccessivamente orientato alla prevenzione dei rischi relativi al trattamento dei dati personali, piuttosto che volti a favorire le imprese per raccogliere le intrinseche opportunità derivanti dall'innovazione digitale, con un conseguente aggravio di costi per le imprese e appesantimento della *user experience*. La conseguenza indesiderata di determinate previsioni normative e regolamentari è quella sia di ostacolare l'innovazione digitale di servizi delle aziende europee rispetto ai loro *competitor* globali, sia di prevenire la nascita di *player* digitali europei in grado di competere con *provider* extra europei.

Gli interventi regolamentari, ove si ravvisi la necessità di stabilire nuove regole ad esempio a protezione dei cittadini, al contrario dovrebbero scongiurare i possibili effetti distorsivi e garantire un *level playing field* a livello globale.

Il fenomeno della *digital economy* può essere analizzato su due dimensioni: innovazione e velocità, dove la componente digitale rappresenta la nuova sintassi, ovvero un elemento dirompente in grado di generare, se indirizzato, un significativo valore con ricadute profonde su produttività e crescita di un paese.

Accenture e *Oxford Economics* hanno elaborato una misura di quello che hanno definito "densità digitale"³ per rapportare il fenomeno della digitalizzazione alla produttività e al PIL per paese, per individuare dove risiedono opportunità e punti di saturazione. Il mercato

³ Accenture Strategy, Digital Density Index – Guiding digital transformation.

italiano risulta essere il fanalino di coda se confrontato ai principali mercati europei, con anche dieci punti di svantaggio rispetto alle più digitali economie del Nord Europa, quantificabile in uno 0,40% di minore produttività e uno 0,25% di minor PIL causato da “insufficiente digitalizzazione del mercato”: bassa connettività, modesto ricorso ai *marketplace*, insufficiente collaborazione in chiave digitale fra le imprese.

Tale svantaggio risulta essere ancor più consistente se alla densità digitale del mercato si somma la densità digitale nell’organizzazione delle imprese, nei modelli di approvvigionamento e nel sistema pubblico economico.

Il framework regolamentare e normativo europeo

Sebbene il regolatore europeo abbia sviluppato una complessa strategia per favorire lo sviluppo del mercato unico digitale e al contempo per facilitare e migliorare l’accesso ai finanziamenti per le piccole e medie imprese attraverso una pluralità di misure e di atti, sussistono tutta una serie di ostacoli alla raccolta e alla condivisione dei dati a livello transnazionale e intersettoriale.

Di seguito elenchiamo quelli che a nostro avviso rappresentano i principali interventi delle istituzioni europee in tema di digitalizzazione nel trattamento dei dati:

- Comunicazione “*Unleashing the Potential of Cloud Computing in Europe*”⁴ del Settembre 2012;
- *European Cloud Initiative*⁵ del Settembre 2012;
- *E-invoicing directive*⁶ dell’Aprile 2014;
- Comunicazione della Commissione al Parlamento EU “*Towards a thriving data-driven economy*”⁷ del Luglio 2014;
- Regolamento europeo in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno⁸ del Luglio 2014;

⁴ *Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>

⁵ Bruxelles, 27.9.2012, COM(2012) 529 final, COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI Sfruttare il potenziale del cloud computing in Europa.

⁶ DIRETTIVA 2014/55/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 16 aprile 2014 relativa alla fatturazione elettronica negli appalti pubblici.

⁷ Bruxelles, 2.7.2014, COM(2014) 442 final, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Verso una florida economia basata sui dati.

- *Opinion* su big data dello *European Data Protection Supervisor*⁹ (di seguito anche EDPS) del Luglio 2015;
- *Digital Single Market (DSM) strategy*¹⁰, una delle priorità della Commissione guidata da Juncker;
- *Draft report on virtual currencies*¹¹ del Febbraio 2016, con particolare riferimento alla *distributed ledger technology* di *blockchain* (della quale si individuano potenziali rischi e ci si interroga su eventuali interventi normative – regolamentari);
- EBA, Discussion Paper “*on innovative uses of consumer data by financial institutions*¹²” di maggio 2016, riguardante gli usi innovativi dei dati sui consumatori da parte degli istituti finanziari. Il documento identifica i rischi e i benefici per i consumatori, per gli istituti finanziari e per l’integrità del mercato in generale riguardante l’utilizzo di tali informazioni raccolte dagli istituti.

EDPS, Article 29 WP e la nuova General Data Protection Regulation

Molte di queste iniziative sono comunicazioni (dalla Commissione al Parlamento / Consiglio ecc.) o Opinioni (dell’EDPS) o iniziative di varia natura: non hanno quindi alcuna ricaduta pratica allo stato attuale, come invece il settore privato si sarebbe aspettato, ad esempio, dalla comunicazione della Commissione *Towards a thriving data-driven economy* del 2014¹³ e della successiva *Opinion* dell’EDPS in materia di big data – quest’ultima sicuramente non invita all’uso di big data, ma dimostra una conoscenza approfondita da parte del Supervisor dei nuovi modelli di data processing e pone delle riflessioni di rilievo.

⁸ REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

⁹ *Opinion 7/2015, Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability.*

¹⁰ http://ec.europa.eu/priorities/digital-single-market_en

¹¹ *Draft report of the Committee on Economic and Monetary Affairs of the European Parliament, Rapporteur: Jakob von Weizsäcker.* <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONGML%2BCOMPARL%2BPE-575.277%2B01%2BDOC%2BPDF%2BV0%2F%2FEN>

¹² Discussion Paper EBA:

https://www.eba.europa.eu/newspress/calendar?p_p_id=8&_8_struts_action=%2Fcalendar%2Fview_event&_8_eventId=1455505

¹³ Tra le azioni individuate dalla strategia della Commissione in materia di big data, si legge infatti la seguente: “*focus public R&I on technological, legal and other bottlenecks*”.

Di fatto, sono evidenti i limiti di un approccio *consumer oriented* che tende ad essere declinato mediante l'imposizione di vincoli alle imprese alla raccolta e utilizzo dei dati. **EDPS e Article 29 Working Party hanno come missione quella di tutelare gli interessati attraverso misure poste a fondamento della protezione del trattamento di dati personali che spesso vanno ben oltre ciò che gli stessi cittadini europei ritengono necessario.**¹⁴ Senza voler entrare nella giustezza di tale missione, il metodo adottato (che può essere definito "giocare in difesa") comporta spesso l'emanazione di **decisioni od opinioni che hanno lo scopo di bloccare, o almeno rallentare, processi di processi di data processing già in corso (anzi, in corsa a livello globale), con l'unico ed indesiderato effetto di svantaggiare player europei rispetto a player extra europei - ma soprattutto senza riuscire ad impostare una strategia della protezione dei dati personali che sia al contempo efficace e sostenibile.**

Così ad esempio la nascente regolamentazione¹⁵ sulla protezione dei dati personali e la direttiva europea sulla tutela dei consumatori¹⁶, attualmente in fase di revisione, pongono dei significativi ostacoli organizzativi ed operativi allo sviluppo e la commercializzazione di nuovi prodotti e servizi. Pur contemplando e riconoscendo il valore intrinseco della *big data analysis*, del *profiling* e di tecnologie a supporto quali *block chain* e *distributed cloud*, tanto da dedicarvi interi capitoli della regolamentazione e delle raccomandazioni agli Stati Membri, **le Istituzioni europee non hanno posto le basi per un superamento univoco e armonizzato delle incertezze relative alla condivisione delle informazioni e l'integrazione dei dati al fine di sviluppare nuove idee di business e nuovi servizi per i cittadini europei.** Non che sia facile: trovare un equilibrio tenendo conto dei nuovi modelli di data processing, delle esigenze di profilazione e dello scarso interesse, salvo subire danno, dei consumatori agli aspetti di protezione dei propri dati è quasi una mission impossible. Ma ci si chiede se 5 anni di lavori per un Regolamento di principi generali siano stati veramente la scelta migliore.

¹⁴ E' una realtà innegabile che i cittadini europei, come quelli del resto del mondo d'altronde, siano disposti a cedere i propri dati personali in cambio di servizi digitali (si pensi ai servizi di *email*, *chat*, e *social in generale*) ed è quindi evidente che la partita da giocare sia quella dell'informazione verso gli interessati più che della protezione da servizi che essi stessi hanno interesse a fruire. E' l'ora di fare i conti con il fatto che i cittadini europei attraverso l'*Internet* e il modello *connected everywhere* sono cittadini del mondo e che, pertanto, i nuovi modelli di consumo di servizi determina una concorrenza globale per le imprese europee che rischiano di restare schiacciate di oltreoceano..

¹⁵ Bruxelles, 25.1.2012, COM(2012) 11 final, Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati).

¹⁶ DIRECTIVE 2011/83/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

Ad oggi interi settori che lavorano su dati personali non sono in grado di prevedere cosa cambierà per loro a breve, all'entrata in vigore del Regolamento¹⁷ e alla scadenza dei termini per l'adeguamento a Maggio 2018 – di conseguenza non possono pianificare per allora i necessari adeguamenti ed investimenti.

Il complesso normativo-regolamentare: una selva oscura

Esistono settori economici che hanno più regolatori, con compiti e competenze diverse, i quali possono individuare ulteriori regole e restrizioni settoriali nell'utilizzo di dati e/o nello sviluppo di servizi innovativi basati sui dati, nonché regolatori e supervisori a livello nazionale e sovranazionale. Si creano in questo modo ambiti di competenza potenzialmente concorrenti fra autorità e organismi indipendenti, multidimensionali tenendo conto anche del livello geografico, che ampliano il livello di incertezza regolamentare in cui le imprese europee ed italiane sono chiamate a prendere decisioni, definire strategie ed pianificare investimenti.

Un esempio prepotente in questo senso è il settore bancario. Tutto bene finché è business as usual; ma cosa succede se una banca intende sviluppare un servizio innovativo, basato su una nuova tecnologia? Quante e quali verifiche deve fare per garantire la compliance multi-livello che le viene richiesta?

Una ricognizione anche delle fonti normative e regolamentari a livello settoriale, anche solo sul settore bancario appena citato, richiederebbe uno sforzo che è fuori scopo rispetto al presente documento: ci basti però tener presente che questo ulteriore livello aumenta di qualche ordine di grandezza la complessità delle regole da tenere in considerazione ogni qual volta si intende sviluppare un nuovo servizio rivolto al cliente finale (o tentare di digitalizzare un servizio esistente).

Entrando nel merito delle previsioni poi, proprio perché ci si confronta con nuovi modelli di business e nuove tecnologie che si affastellano a ritmi sempre crescenti, il vero rischio è quello di non riuscire a definire regole certe. Per fare un recente esempio nel settore bancario, possiamo citare il *Discussion Paper on Automation in Financial Advice* del *Joint*

¹⁷ Un esempio emblematico sotto questo profilo è quello del settore dei *credit reporting service provider*. La direttiva 95/46/CE del Parlamento europeo e del Consiglio fu recepita in maniera molto disomogenea a livello di singoli Stati Membri, tanto che ad oggi il *credit reporting* non si basa nemmeno sugli stessi *legitimate grounds*. Alcune Data Protection Authority (DPA) hanno addirittura impedito la creazione nel proprio Stato Membro di *credit bureau* privati, o lo scambio di dati a livello *cross border*. ACCIS, l'associazione europea di settore, non ha ricevuto risposte sugli impatti effettivi del regolamento dal livello europeo (EDPS), che ha rimandato alle DPA nazionali per una prima analisi.

*Committee European Supervisory Authorities (ESAs)*¹⁸. Senza addentrarsi, basti anche solo citare che una delle 3 caratteristiche individuate da EBA per identificare l'*automated advice* è che l'*advice* sia percepito come tale dal cliente ("*The output of the tool is, or is perceived to be, financial advice*"). Nel 2016 è da considerarsi perlomeno inaccettabile un tale livello di pressapochismo definitorio da parte di Autorità sovranazionali, per quanto a livello di discussion paper. È chiaro che anche qui, come per la data protection, è difficile individuare un ambito oggettivo che sia sufficientemente ampio - ma non troppo, così da ricomprendere tutte le nascenti forme di *robo-advice* e possibilmente anche quelle che verranno, ma non per questo può essere creata incertezza giuridica a priori.

Bitcoin, blockchain e DLT

Lo scenario non è comunque totalmente negativo: il fatto che il Parlamento europeo stia iniziando ad interrogarsi su opportunità e rischi della tecnologia *blockchain* è sicuramente un elemento incoraggiante¹⁹. Peraltro, nel documento si tratteggia come la DLT può essere una tecnologia per risolvere nativamente (in linea a con la chiamata alle tecnologie "*privacy by design*" dell'EDPS nella citata *Opinion*²⁰) il problema di garantire livelli differenziati di riservatezza nel trattamento di dati personali. È di pochi giorni fa²¹ la notizia che **l'Unione Europea ha deciso di soprassedere per il momento e di non intervenire con un'iniziativa regolamentare sulle tecnologie Blockchain**, per non rischiare di porre vincoli prematuri allo sviluppo della sperimentazione applicativa.

Elemento incoraggiante, anche se occorrerà monitorare da vicino i *lawmakers* globali (in particolare in US, UK e in Asia) e accompagnare il processo regolatorio europeo per sperare che sia tempestivo ed efficace nei contenuti, anche a vantaggio delle industry europee.

A livello globale, questi i passi compiuti sinora:

¹⁸ <https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/discussion-paper-on-automation-in-financial-advice/-/regulatory-activity/discussion-paper>. Val la pena anche notare che EBA dedica un'intera pagina del proprio sito a raccogliere le disposizioni in materia di *Consumer protection and financial innovation*.

¹⁹ *Draft report of the Committee on Economic and Monetary Affairs of the European Parliament, Rapporteur: Jakob von Weizsäcker*. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONGML%2BCOMPARL%2BPE-575.277%2B01%2BDOC%2BPDF%2BV0%2F%2FEN>

²⁰ *Opinion 7/2015, Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability*.

²¹ <http://www.newsbtc.com/2016/04/26/european-union-pushes-away-bitcoin-regulation-for-now/>. L'articolo cita che anche la BCE stia sperimentando la tecnologia, così come il seguente articolo esplicita l'interesse del Governo britannico a valutare l'adozione della tecnologia blockchain nella distribuzione di grants e student loans: <http://disruptiveviews.com/british-government-exploring-blockchain-for-money-distribution/>

- Gennaio 2016: l'**IMF** ha pubblicato un report circa benefici e rischi dei distributed ledgers affermando che arrivare a un framework normativo bilanciato che protegge contro i rischi senza soffocare l'innovazione è una sfida che richiederà intensa collaborazione a livello internazionale²².
- Febbraio 2016: il **FSB**, che stabilisce i global standards per i Paesi del G20, ha annunciato che farà un assessment delle innovazioni fintech innovations, ivi compresa la DLT, per assicurare che il framework regolamentare sia in grado di gestire i rischi sistemici senza limitare l'innovazione²³.
- Febbraio 2016: Christopher Woolard, Director of Strategy and Competition dell'**FCA**, ha dichiarato che l'**FCA** sta monitorando gli sviluppi tecnologici, ma che non farà mosse fino a quando le sue applicazioni non saranno più chiare²⁴. L'approccio che l'**FCA** adotterà è quello del **Regulatory Sandbox**: ***"The Sandbox will allow businesses to test out new, innovative financial services without incurring all the normal regulatory consequences of engaging in those activities. [...] We will offer a range of options for firms such as authorisation for testing; [...] Safeguards for consumers and the financial system while testing will be agreed between the businesses and the FCA. One thing that we won't compromise is lower standards of protection for consumers."*** In particolare riguardo alla DLT, l'**FCA** intende lavorare con le aziende per sviluppare soluzioni *distributed ledger* attraverso Project Innovate (Hub di Innovazione lanciato ad Ottobre 2014 e che ha concretamente aiutato la nascita di nuove aziende in ambito financial services in UK) per assicurare che le protezioni per i consumatori siano previste già nella fase di implementazione della tecnologia (*privacy by design*).

L'approccio dell'FCA**, ribadito in varie occasioni anche dal Governo britannico è sicuramente da guardare con interesse e da considerare come benchmark anche per altri Paesi europei, Italia compresa, in quanto consente:**

- alle aziende, di sentirsi libere di sperimentare senza doversi assumere eccessivi rischi di compliance, o attendere per mesi autorizzazioni per progetti di R&S che non hanno ancora comprovate ricadute per definizione.

²² Virtual Currencies and Beyond : Initial Considerations – 20 Gennaio 2016

<http://www.imf.org/external/pubs/cat/longres.aspx?sk=43618>

²³ Letter of the FSB' Chairman to G20 Finance Ministers and Central Bank Governors- 22 Febbraio 2016

<http://www.fsb.org/wp-content/uploads/FSB-Chair-letter-to-G20-Ministers-and-Governors-February-2016.pdf>

²⁴ "UK FinTech: Regulating for innovation ", speech by Christopher Woolard, delivered at the FCA's event on UK FinTech: Regulating for innovation on 22 February 2016 <https://www.fca.org.uk/news/uk-fintech-regulating-for-innovation>

- All'authority, di poter da una parte non perdere il controllo di quello che sta succedendo in termini di evoluzione innovativa, dall'altra di poter integrare nuove progettualità con i presidi di tutela che è chiamata a garantire come authority ed infine di individuare il momento giusto per un intervento di guidance, soft o hard regulation.
- Ai consumatori infine, di sentirsi in ogni caso tutelati da un'authority che ha una strategia chiara e di lungo periodo, proprio perché parte dal concepimento stesso delle nuove tecnologie.

Digital Single Market Strategy

La *Digital Single Market Strategy - Bringing down barriers to unlock online opportunities* - è una delle priorità della Commissione europea di Juncker²⁵. I 3 pilastri su cui si fonda sono:

- favorire un migliore accesso ai consumatori e alle imprese ai beni e ai servizi online in Europa;
- creare le giuste condizioni per lo sviluppo delle reti digitali e dei servizi;
- massimizzare il potenziale di crescita dell'economia digitale europea.

La struttura di questa strategia, rappresentata da un *mix* di iniziative e proposte legislative in parte ancora da venire, non ha sorpreso gli *stakeholder*, alcuni dei quali rivedono nelle nuove proposte della Commissione la scarsa ambizione che ha spesso caratterizzato le passate iniziative in ambito digitale (dai *CEOs roundtable summits* del 2011, al piano di azione per *l'e-commerce* del 2012, al Continente Connesso – ridotto ormai alle due sole misure del *roaming* e *net neutrality*) spesso bloccate o fallite per mancanza di un accordo politico.

Le perplessità vengono in particolare delle piccole imprese ad alto tasso innovativo - che temono una deriva regolamentare che potrebbe intralciare anziché sostenere l'economia digitale europea - e dalle grandi imprese, che chiedono un'implementazione rapida delle regole utili ad avere un level playing field chiaro e definito.

In un recente comunicato²⁶, la Commissione europea ha tracciato i progetti che intende implementare per aiutare l'industria europea, le PMI, i ricercatori e le autorità pubbliche a

²⁵ La pagina dedicata alla DSM strategy: https://ec.europa.eu/priorities/digital-single-market_en

trarre il massimo vantaggio dalle nuove tecnologie. In particolare per l'industria privata, la Commissione propone di definire rapidamente **norme tecniche** finalizzate a garantire l'interoperabilità transnazionale su cinque settori prioritari: 5G, cloud computing, **internet of things, data technologies** e **cybersecurity**. Il processo di setting delle norme tecniche sarà accelerato grazie al **cofinanziamento di test e sperimentazioni** delle predette tecnologie, anche attraverso partenariati pubblico-privato: non siamo al *Regulatory Sandbox* dell'FCA, la strada è buona ma servirebbe più coraggio nell'affrontare le sfide poste dalle nuove tecnologie.

Identificazione elettronica

I principali fattori che hanno portato a redigere il regolamento in materia di identificazione elettronica²⁷ sono:

- **Campo di applicazione ristretto del quadro giuridico preesistente:** I servizi eIAS sono indispensabili per un'ampia gamma di interazioni elettroniche come i servizi bancari (eBanking), l'amministrazione in linea (eGovernment) e i servizi sanitari online (eHealth). A livello UE esiste un quadro regolamentare limitato essenzialmente alle firme elettroniche.
- **Assenza di coordinamento fra lo sviluppo delle firme elettroniche e dell'eID:** l'assenza di riconoscimento e di accettazione reciproci e l'interoperabilità sono tra i problemi più rilevanti sia per gli utilizzatori che per i prestatori di servizi. anche se il problema dovrebbe essere superato almeno in parte con la piena entrata in vigore del Regolamento eIDAS il 1 Luglio 2016 (dato che il regolamento dovrebbe garantire che cittadini e imprese possano utilizzare lo schema di identificazione elettronica usato a livello nazionale per accedere a servizi – pubblici – in altri Stati Membri nei quali le identità elettroniche esistono).
- **Assenza di trasparenza delle garanzie di sicurezza:** gli utilizzatori percepiscono la mancanza di sistemi sicuri di eID come una barriera all'ingresso. La sicurezza deve essere garantita sia sul processo di identificazione del soggetto fisico al quale viene associata una eID, sia sul trattamento dell'eID e sulla conservazione di dati personali (ed eventualmente biometrici) utilizzati per l'identificazione.

²⁶ Un percorso per la digitalizzazione dell'industria europea, 19 Aprile 2016 http://europa.eu/rapid/press-release_IP-16-1407_it.htm

²⁷ Regolamento (UE) N. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. Così detto Regolamento eIDAS

- **Scarsa informazione e adesione da parte degli utilizzatori:** gli utilizzatori finali, che generalmente non dispongono di conoscenze sufficienti, devono potersi affidare a regole che stabiliscano chiari diritti e responsabilità per tutte le parti interessate (prestatori di servizi fiduciari, utilizzatori finali e organismi di *governance*).
- **Limitazioni europee nazionali all'utilizzo di dati biometrici per facilitare sistemi di riconoscimento a distanza efficaci per il rilascio di eID:** basti pensare che le stesse Certification Authorities che emettono eTS²⁸, oltre ad avere un'approvazione del proprio processo da parte dell'AgID in Italia, devono fare prior checking con l'Autorità Garante nel caso in cui il processo preveda l'utilizzo di dati biometrici (es. video con registrazione del volto, file audio con registrazione della voce, etc.), a meno che non adottino processo già precedentemente approvato.

Con l'evoluzione del commercio internazionale e la "virtualizzazione" dell'accordo telematico, anche nell'ambito degli accordi privatistici il sistema tradizionale legato alla visione del documento - quale *res rappresentativa di un fatto*, imputabile giuridicamente attraverso la sottoscrizione - è entrato irrimediabilmente in crisi e si è pertanto reso indispensabile trovare nuove nozioni più elastiche di documento che tenessero conto delle innovazioni della prassi e rendessero giuridicamente ammissibili le moderne tecniche di attribuzione della paternità dello "scritto", prescindendo dai meccanismi tipici legati alla sottoscrizione. Ovviamente la parificazione di un documento informatico alla "forma scritta" pone problemi innegabili e simili a quelli già noti relativi alla rilevanza formale e probatoria. Tali problematiche devono essere risolte cercando di tenere separati gli ambiti legati alle esigenze di "certificazione", tipici dei rapporti della P.A., da quelli dell'e-commerce internazionale.

Le più sofisticate e importanti elaborazioni dottrinali in materia di contrattualistica comunitaria e internazionale: *The Principles Of European Contract Law 2002*²⁹ e *The UNIDROIT Principles of International Commercial Contracts*³⁰ unitamente ai Principi di diritto europeo dei contratti (PECL) possono essere considerati come il più prestigioso e riuscito "esperimento di codificazione" di un emergente regime giuridico sovranazionale e comunitario delle "transazioni" internazionali. Il legislatore comunitario ha, quindi, considerato - per quanto riguarda nello specifico il documento informatico - la categoria "firma elettronica" prescindendo dalla "tecnica" utilizzata per creare l'associazione del

²⁸ Namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication

²⁹ <http://www.jus.uio.no/lm/eu.contract.principles.parts.1.to.3.2002/toc>

³⁰ <http://www.unidroit.org/english/principles/pr-main.htm>

documento al suo titolare e questo con l'ovvia intenzione di lasciare libertà ai privati, in modo che si possano trovare nel tempo anche nuove soluzioni tecnologiche più appropriate alle esigenze della prassi commerciale³¹.

E in Italia?

La mancanza di ambizione della normativa europea si riverbera inevitabilmente sul livello nazionale. Questo crea delle frizioni nei rapporti con gli utilizzatori finali dei servizi che presuppongono il trattamento dei dati personali.

A livello italiano ci si riferisce in particolare ai seguenti interventi normativi:

- Codice Amministrazione Digitale³² e nodo dei pagamenti;
- Disposizioni in materia di fatturazione elettronica verso la Pubblica Amministrazione³³;
- Sistema Pubblico per la gestione dell'Identità Digitale (SPID)³⁴, abbattendo i costi di ingresso e quelli di accreditamento degli utenti, dovrebbe, secondo le aspettative del Governo, veicolare rapidamente le imprese al trasferimento della propria attività commerciale sul web. Il sistema SPID è un sistema ad attuazione graduale, in

³¹ La firma elettronica, si ricorda, è definita dal legislatore italiano come l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 2, lett. a, d.lgs. 10/2002). Per la firma elettronica leggera non sono previsti, pertanto, dal legislatore sistemi di validazione e di certificazione (necessari, invece, per le firme elettroniche avanzate). I cd. metodi di autenticazione informatica sono invece genericamente tutto quell'insieme di strumenti elettronici e delle procedure per la verifica indiretta dell'identità, secondo la definizione fornita dal D.Lgs. 196/2003 all'art. 4 comma 3 lett. c) - quali ad esempio, l'uso di password o di codici di identificazione personale, così come qualsiasi altro metodo che permetta in maniera diretta (o indiretta) un'identificazione (a prescindere da qualsiasi valutazione sulla sicurezza di quella identificazione, perché tali valutazioni riguardano il profilo probatorio e sono, quindi, affidate al prudente apprezzamento del giudice). E, infatti, il significato "tecnico" e generalmente accettato di sistemi di authentication per le firme elettroniche è: "A technical definition of authentication is the process of establishing whether someone or something is who or what its identifier states it is. An authentication process may be enabled by: (i) something you know, like a PIN or password; (ii) something you have, as with smartcards, challenge-response mechanisms, or public-key certificates; (iii) something you are, as with positive photo identification, fingerprints, and biometrics".

³² Decreto Legislativo 7 marzo 2005, n. 82

³³ LEGGE 24 dicembre 2007, n. 244 Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2008)

³⁴ Primo provvedimento di attuazione previsto dall'articolo 64, comma 2-sexies del D.lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) è il decreto della Presidenza del Consiglio dei Ministri 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014. Il 28 luglio 2015, con la Determinazione n. 44/2015, sono stati emanati i quattro regolamenti previsti dall'articolo 4, commi 2, 3 e 4, dell' suddetto DPCM 24 ottobre 2014. Il regolamento che norma le modalità di accreditamento entra in vigore il 15 settembre 2015, data dalla quale i soggetti interessati possono presentare domanda di accreditamento all'Agenzia. Ai fini della trasmissione all'Agenzia della documentazione è stato reso disponibile il certificato contenente la chiave per criptare la documentazione riservata. Con l'emanazione dei suddetti regolamenti il Sistema Pubblico di Identità Digitale diviene operativo.

due fasi. La prima fase si concluderà il 15 giugno 2016, mentre la seconda entro i successivi 24 mesi³⁵;

- Provvedimento con cui il Garante per la protezione dei dati personali ha vietato l'uso di un sistema di riconoscimento facciale che avrebbe dovuto registrare e verificare i volti di chi richiede un finanziamento allo scopo di prevenire possibili furti di identità³⁶;
- Posizione italiana su Mercato Unico digitale³⁷ (vedi anche appendice al presente documento);
- Atti di recepimento della normativa europea sugli Open data³⁸.

In materia di **identità digitale** è stata avviata di recente la procedura di rilascio delle ID Digitali (identità digitali) da parte degli *Identity Provider*, soggetti accreditati in grado di dare concreta attuazione alla “digitalizzazione del Paese”. Lo scopo è quello di garantire la certezza dell'identità delle persone nelle transazioni digitali. In questo modo i cittadini potranno accedere con una sola identità telematicamente a tutti i servizi erogati dalle pubbliche amministrazioni e dalle imprese che adotteranno il sistema. L'idea alla base è semplice: un PIN unico che consentirà ai singoli utenti di accedere e adoperare i servizi *online* del circuito SPID di Comuni, enti previdenziali (come l'INPS), Agenzia delle Entrate, evitando le code agli sportelli e di incappare in eventuali frodi. Il **Sistema Pubblico per la gestione dell'Identità Digitale** (di seguito anche SPID)³⁹ è un insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia Digitale (di seguito anche AgID), gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto

³⁵Il Direttore Generale di AgID Antonio Samaritani, in occasione della sua audizione in Commissione Anagrafe Tributaria, ha dichiarato: “[...] In linea con la previsione normativa che obbliga le PA ad utilizzare SPID ma prevede la possibilità di utilizzo da parte dei privati, SPID può essere un fondamentale volano per lo sviluppo e soprattutto l'utilizzo dei servizi digitali da parte dei cittadini. Infatti una user experience comune, le stesse credenziali valide per tutti i fornitori di servizi pubblici e privati e la vigilanza dello Stato, aumentano, come diversi studi confermano, la fiducia e la propensione all'utilizzo dei servizi digitali. Inoltre startup e imprese innovative, purtroppo poco presenti in internet rispetto alla media UE, possono utilizzare una base utenti già identificata e dotata di credenziali di accesso senza doversi preoccupare di investire in queste attività. Quindi la Pubblica Amministrazione come volano per lo sviluppo digitale, infatti già oggi il numero di interazioni che richiedono autenticazioni effettuate verso i privati è enormemente superiore a quelle che un cittadino effettua verso le PA. Tra i settori privati quelli che hanno mostrato il maggiore interesse verso SPID sono: bancario, assicurativo, trasporti, media, shared economy. [...]”

³⁶ Verifica preliminare. Sistema di riconoscimento facciale delle fotografie poste sui documenti di identità di soggetti che abbiano presentato a banche ed intermediari finanziari richieste di finanziamento, da utilizzare per prevenire furti di identità - 25 febbraio 2016, Registro dei provvedimenti n. 77

³⁷ Position paper del governo italiano sul Mercato unico digital,

http://www.sviluppoeconomico.gov.it/images/stories/pubblicazioni/Position_paper_on%20DSM_ITALIA.pdf

³⁸ DECRETO LEGISLATIVO 18 maggio 2015, n. 102, Attuazione della direttiva 2013/37/UE che modifica la direttiva 2003/98/CE, relativa al riutilizzo dell'informazione del settore pubblico.

³⁹ Vedi anche infra paragrafo successivo.

delle pubbliche amministrazioni. Secondo quanto riportato nel sito dell'AgID, SPID riguarda l'accesso non solo ai servizi online della PA, ma anche ai servizi dei privati aderenti al sistema (tra le motivazioni di SPID presentate dall'Agenzia vi è quella di "incrementare l'utilizzo dei servizi *online*, specialmente quelli dispositivi e il commercio elettronico, in maniera da risalire le posizioni nello scenario EU e beneficiare dell'utilizzo di internet e delle nuove tecnologie in tutti i settori economici"). **Dal 15 marzo 2016 i primi tre gestori di identità digitale accreditati da AgID rendono disponibili le prime identità digitali.**

La società Infocert insieme a Poste e Telecom, è stato uno dei primi gestori accreditati per l'identità digitale. Attraverso InfoCert, la procedura di assegnazione dell'identità digitale al singolo cittadino può avvenire anche tramite riconoscimento tramite *webcam*⁴⁰. Il video, oltre ai dati richiesti, prevede la scansione in tempo reale a distanza di un proprio documento di identità e dei dati anagrafici. Infocert è stata autorizzata dal Garante Privacy con provvedimento del 24 settembre 2015: "Processo di rilascio con riconoscimento a mezzo webcam" per firma elettronica qualificata o digitale e, a tal fine, ha prescritto alla Società istante, ai sensi dell'art. 17 del Codice: – di esplicitare nell'informativa da fornire ai richiedenti, ai sensi dell'art. 13 del Codice, le modalità di riconoscimento alternative; – di predisporre, per maggiore tutela e sicurezza dei dati, misure di cifratura per tutti i documenti e i file audio/video inviati in conservazione; – di limitare la registrazione del flusso audio/video alla esibizione del documento di identità e all'interazione con l'operatore nella parte in cui viene documentata la reale volontà del richiedente di ottenere un certificato di firma digitale.

Recentemente le Commissioni riunite Trasporti e Attività produttive della Camera dei deputati hanno avviato un ciclo di audizioni proprio con riferimento all'attuazione della **strategia sul mercato unico digitale e sull'e-commerce** e ai relativi atti dell'Unione europea. Si sono svolte finora le audizioni del Presidente dell'AGCM Pitruzzella, del Presidente Agcom Prof. Cardani, del Presidente Garante Privacy Soro e della dottoressa Simonetta Montemagni, Direttrice di ricerca dell'Istituto di linguistica computazionale "Zampolli" del CNR. In particolare il Presidente Soro nell'ambito del suo intervento in audizione ha sottolineato i pericoli insiti nelle attività di profilazione legate alle attività del mondo *online*, dei siti *e-commerce*, dei *social network* e dei motori ricerca da cui le aziende traggono enormi vantaggi di carattere economico. In tale contesto ha evidenziato un problema di scarsa responsabilità diffusa da parte degli utenti che rilasciano spesso il

⁴⁰ Trattamento di dati personali nell'ambito del "Processo di rilascio con riconoscimento a mezzo webcam" per firma elettronica qualificata o digitale. Verifica preliminare - 24 settembre 2015, Registro dei provvedimenti n. 491

consenso in modo incauto, auspicando un dibattito pubblico sul tema dei *big data* che possono rendere identificabile un soggetto che non ha lasciato il consenso al trattamento dei propri dati. Il Presidente Soro ha in qualche modo escluso che i cittadini europei possano consapevolmente cedere i propri dati consapevolmente e per ottenere in cambio i vantaggi derivanti dalla fruizione dei servizi digitali, al contrario ha individuato nella direttiva sui contenuti - nella parte in cui prevede anche una controprestazione non pecuniaria sotto forma di dati personali ceduti dagli utenti - una violazione di un diritto fondamentale riconosciuto dai trattati.

John Phelan ha usato una metafora per fare il punto della situazione. ***“Ora è come avere 28 diverse serrature sulla porta di un mercato unico digitale, una per ogni Paese dell’Ue. Si tratta di un problema di lunga data. È necessario che l’Unione europea utilizzi questa strategia come trampolino di lancio per dimostrare il coraggio politico e normativo per superare gli interessi commerciali che oggi frenano l’accesso per i consumatori europei a tutti i contenuti digitali”***.

Wrap up

Per giocare ad armi pari la partita dell’innovazione con i *player* extra europei, è indispensabile rimuovere le barriere esistenti all’utilizzo e all’integrazione dei dati che sono alla base del funzionamento delle c.d. *disruptive innovations*, nonché i profili di incertezza giuridica che ostacolano la pianificazione e l’investimento in *business* innovativi ed applicazioni rivoluzionarie. Queste sono condizioni imprescindibili per una società che intenda generare valore e benessere per i propri cittadini.

E non sono sufficienti: oltre a questo, serve ripensare il modo con cui i legislatori affrontano l’innovazione. Non reagire e arginare, bensì accompagnare e stimolare una crescita in linea con i principi della Carta Dei Diritti Fondamentali Dell’unione Europea⁴¹.

Ecommerce, digital marketing, social media, stampanti 3D, cloud, Internet of things, analytics, droni, realtà aumentata, crowdfunding, cybersecurity, blockchain e sharing economy sono alcune delle innovazioni che si sono affacciate sul mercato e molte altre non sono ancora immaginabili, nei quali e tra i quali le tecnologie sono fattori abilitanti

⁴¹ <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A12012P%2FTXT>

formidabili. Si tratta di innovazioni trasversali a svariati settori di attività e il cui potenziale, in termini di valore aggiunto, è direttamente correlato alla possibilità di utilizzare ed incrociare grandi moli di dati per finalità di business. Tale è il valore di questi servizi, prodotti e tecnologie e tale è il beneficio per la vita di cittadini, che essi stesso sono sempre più disposti a mettere a disposizione i propri dati personali al fine di ottenere in cambio prodotti e servizi sempre più flessibili ed adatti alle loro specifiche esigenze.

Il bilanciamento tra protezione dei dati e innovazione non può più essere trovato attraverso un approccio quantitativo: il sistema di valutazione è complesso e deve tener conto l'effettivo rischio di compressione del diritto alla riservatezza da una parte e i benefici economici e sociali di un dato modello di business data driven. Né tale bilanciamento può essere ancora gestito con meccanismi come prior checking e valutazione giurisprudenziale: i ritmi evolutivi non consentono questi tempi, pena un ritardo incolmabile del time to market sui competitor extra europei.

Si tratta di una sfida complessa per le imprese e le autorità europee, in cui la posta in gioco non è la sola quota di mercato, ma la vera e propria sopravvivenza del *business* in un ecosistema interconnesso e senza frontiere. Tuttavia sembra che ad oggi in Europa ed in Italia sussista l'illusoria convinzione di poter proteggere i cittadini imponendo vincoli e restrizioni che hanno invece l'effetto di disincentivare gli investimenti e l'innovazione. E' storica l'affermazione di Benjamin Franklin "*Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety*"⁴².

Dobbiamo fare i conti con un mondo extra UE, come Stati Uniti e Asia, dove le autorità di regolazione del settore bancario stanno sviluppando modelli di collaborazione pubblico-privato atti a favorire le innovazioni in ambito *fintech* e di incentivazione degli investimenti in *start up fintech*⁴³. L'Europa rischia di perdere un treno che non ripasserà e di lasciare le imprese di casa propria al palo nella corsa all'innovazione, nascondendosi dietro false istanze di sicurezza che gli stessi cittadini fanno fatica a concepire nel momento in cui si vedono negato l'accesso a contenuti e servizi di maggiore qualità, o offerti a migliore condizioni e maggiormente customizzati sulle loro esigenze.

I regolatori europei dovranno trovare le risposte alle seguenti domande:

- in un sistema distribuito, chi o cosa dovrà essere regolato?

⁴² Dalla Risposta al Governatore, Assemblea della Pennsylvania, 11 novembre 1755; in The Papers of Benjamin Franklin, ed. Leonard W. Labaree, 1963, vol. 6, p. 242.

⁴³ <https://www.finextra.com/newsarticle/28667/us-regulator-considers-new-framework-for-fintechs>

- considerata la natura *cross-border* della tecnologia, quale organo / istituzione sarà incaricato di definire le regole?
- in che modo si dovrà reimpostare l'impianto definitivo e di classificazione?
- in che modo si garantirà la tutela dei consumatori? Data la complessità della tecnologia sottostante, in che modo ci si assicurerà che abbiano compreso le condizioni dei servizi cui aderiranno?

In ultima analisi l'approccio della britannica FCA (Regulatory Sandbox) ci sembra quello che meglio possa garantire il giusto equilibrio tra sicurezza e libertà, in un mondo in cui l'unico modo in cui le autorità hanno modo di mantenere il controllo sull'evoluzione è quello di instaurare un rapporto strettissimo con le imprese e tracciare con loro (non per loro) la strada verso il domani, sostenendo ed incoraggiando la sperimentazione su quelle tecnologie che di per sé agevolano il presidio della sicurezza.

Appendice: Posizione Italiana sul mercato unico digitale

1) Migliorare l'interoperabilità e valorizzare l'e-commerce:

- definizione di un quadro normativo armonizzato per la costituzione e la registrazione on-line delle imprese, anche transfrontaliera;
- omogenizzare le norme a tutela del consumatore, sulla garanzia dei prodotti e armonizzazione fiscale che allinei le aliquote IVA dei prodotti digitali;
- piattaforma per il pagamento dell'IVA che incentivi l'ingresso sul mercato delle PMI.

2) Accesso a internet veloce e superveloce, alta velocità nel 2020:

- favorire gli investimenti pubblici e privati sulle infrastrutture digitali e sviluppare la banda ultra-larga;
- procedere con la revisione della Direttiva "Servizio Universale" (ad esempio fissando un valore minimo di banda garantito a tutti i cittadini UE);
- sviluppo delle comunicazioni mobili giungendo alla fine del *roaming* in tempi ragionevoli;

3) *Internet governance* e fiducia consumatori: migliorare sicurezza e garanzie:

- ogni Stato Membro individua una autorità nazionale competente che favorisca la cooperazione tra i *Computer Emergency Response Teams (CERT/CSIRT)*;
- rapida approvazione della direttiva Network and Information Security (NIS);
- a garanzia dei consumatori è desiderabile che l'Unione sviluppi un sistema "privacy by default", ad esempio attraverso l'identità digitale, il marchio digitale e l'informazione preventiva di tutti gli operatori.

4) L'industria creativa: sostenere il diritto d'autore *on-line* e l'audiovisivo:

- scelta del regime giuridico in base al criterio del paese di origine dell'*uploading* o a quello di destinazione;

5) Ricerca e Innovazione: liberare il potenziale innovativo attraverso il nuovo modello di manifattura digitale e le *start up*:

- innovazione in chiave *Industry 4.0*, ovvero investimenti in sistemi digitalizzati e interconnessi che favoriscono l'efficientamento dei processi e l'innovazione di prodotto, anche tramite strumenti come quelli offerti da *Internet of Things (IoT)* caratterizzati da maggiore velocità, scambio di dati e informazioni con il cliente finale;
- aumentare la collaborazione e l'integrazione fra imprese e start-up ad alto contenuto innovativo capaci di sviluppare un modello di *open innovation* flessibile e funzionale al modello di manifattura digitale;
- transazione a modelli basati sul sostegno diretto all'impresa. Creazione di strumenti finanziari capace di favorire l'accesso al credito e agli investimenti (come *equity crowdfunding*, la garanzia pubblica sui prestiti bancari e gli incentivi agli investimenti in capitale di rischio);
- realizzazione di un registro comune delle *start up* innovative al fine di consentire la misurazione e il monitoraggio del fenomeno su scala europea;
- strategia comune sui visti, in favore di talenti extra-Ue al fine di trasformare l'Europa in una grande *hub* dell'innovazione incentivando lo scambio di *best practice* e *benchmarking* e diffusione della conoscenza.

6) Migliorare l'alfabetizzazione, le competenze e l'inclusione nel mondo digitale:

- alfabetizzazione digitale, per accrescere le competenze complessive dei consumatori e di conseguenza il mercato per le imprese.

7) *E-government* e infrastrutture digitali: modernizzare il settore pubblico e la rete digitale, *Big Data* e *Cloud Computing*:

- aumentare gli sforzi in materia di sanità digitale, scuola digitale, giustizia digitale, fatturazione elettronica ed anagrafe della popolazione residente;
- *public procurement* digitale, eliminando gli ostacoli presenti derivanti dalla mancanza di standardizzazione e di interoperabilità delle piattaforme telematiche;
- maggior dialogo tra le Pubbliche Amministrazioni europee rafforzando strumenti come l'*internal market information system*, l'ERP per la gestione integrata, il CRM per le relazioni con i cittadini;
- sviluppo di una economia basata sui dati e sul *cloud computing*;

- adozione in Europa della Carta degli open data che dovrà tener conto delle esigenze di natura industriale.