Convegno

VERSO L'ISOLA DEL TESORO
Le rotte dei consumatori tra protezione e mercato e la mappa della regolazione

Roma, 12 dicembre 2017

Documento di output

Piazza dei Santi Apostoli 66, 00187 Roma
Ph. +39 06 4740746 - Fax +39 0640402523
info@i-com.it - www.i-com.it
Rond Point Schuman, 6 - 1040 Bruxelles Tel. + 32 (0) 22347882

INTRODUZIONE

Il presente documento persegue la finalità di sintetizzare e porre in luce le principali evidenze emerse in occasione del **Convegno "VERSO L'ISOLA DEL TESORO. Le rotte dei consumatori tra protezione e mercato e la mappa della regolazione**" tenutosi lo scorso 12 dicembre 2017, nell'ambito del quale è stato presentato l'**Osservatorio Consumatori I-Com 2017**.

La **rivoluzione digitale** in atto sta travolgendo ogni aspetto del nostro vivere quotidiano; ogni ambito, da quello più superficiale a quello più intimo e personale, sembra ridisegnato dalla tecnologia e dai servizi digitali di nuova generazione che, se da un lato, ci offrono nuove straordinarie opportunità e nuovi strumenti di azione (si pensi agli enormi benefici connessi alla diffusione dell'**IoT**, dei **Big Data** e dell'**Intelligenza Artificiale**), dall'altro, ci pongono di fronte a nuove sfide e criticità, da affrontare (prime tra tutte, per rilevanza, quelle connesse alla tutela della sicurezza dei dati).

L'Osservatorio Consumatori 2017, dunque, si è proposto di descrivere il livello di penetrazione del digitale nelle abitudini dei cittadini/consumatori e nel business delle aziende, per poi focalizzare l'attenzione sulle opportunità di sviluppo e le nuove sfide poste dai Big Data e dall'intelligenza artificiale. Infine, l'Osservatorio si è soffermato sul tema della privacy e sicurezza nel cyberspace, con l'obiettivo di indagare quali forme di tutela è necessario mettere in atto affinché imprese e consumatori possano ampiamente utilizzare strumenti e tecnologie digitali e cogliere i numerosi vantaggi che scaturiscono dalla rivoluzione in atto.

I-GROUP 1 - I potenziali benefici dei big data e dell'intelligenza artificiale per consumatori e imprese e le sfide della regolazione

In un contesto sempre più incentrato su Internet e sull'utilizzo dei device mobili si assiste alla produzione di una quantità di dati senza precedenti. Secondo l'OCSE, a fine 2017, il traffico dati avrà raggiunto quota 120 exabyte (miliardi di Gigabyte). Questa enorme esplosione di dati ha fatto sì che uno dei termini ormai ricorrenti sia "**Big Data**", che si differenziano dagli altri dati per la particolare estensione della quantità di dati raccolti (**volume**), la continua evoluzione dei dati e la rapidità di analisi in tempo reale effettuata tramite l'utilizzo di complessi algoritmi (**velocità**) e la diversità e ricchezza a seconda del contenuto e del formato dei dati (**varietà**). Tali dati stanno diventando essenziali per la crescita economica, l'offerta di servizi innovativi, la creazione di posti di lavoro.

Secondo i dati IDC, il **valore di mercato dei dati ammontava nel 2016, solo in Italia, a complessivi 4,6 miliardi di euro** (circa l'8% del totale UE) e dovrebbe superare i 6,3 miliardi di euro da qui al 2020, crescendo quindi ad un tasso medio annuo dell'8,3%.Non solo: la cosiddetta economia dei dati – ossia l'impatto complessivo che il mercato dei dati genera sull'economia, includendo tutta la filiera che li riguarda – impatta sull'economia italiana per un importo pari a 28,4 miliardi di euro, ossia l'1,52% del PIL nazionale. Per quanto riguarda i settori che maggiormente producono dati,

manifatturiero, servizi finanziari e servizi professionali spiegano oltre la metà del valore di mercato complessivo.

Il potenziale è enorme e appare assolutamente necessario usarlo. Sono, infatti, tante e ormai ampiamente riconosciute le **opportunità connesse a questo nuovo "fattore produttivo": un impiego più efficiente delle risorse, un valido ed efficace sostegno al decision-making aziendale, la capacità di rispondere rapidamente ad una domanda in continuo cambiamento - verso ed attraverso una customizzazione di massa - e la creazione di catene del valore sempre più competitive**. Uno dei principali canali di miglioramento della produttività aziendale è la riduzione dei costi operativi grazie alla precoce identificazione di errori o malfunzionamenti nei processi produttivi, rendendo il potenziale in quest'area di più facile raggiungimento. Tuttavia, il maggior potenziale associato ai Big Data va ricercato nel cosiddetto **Data-to-Management**, la cui realizzazione richiede un cambiamento notevole in quello che è il data-driven decision-making all'interno delle imprese europee e, dunque, uno sforzo organizzativo importante e di difficile applicazione.

Nonostante l'inesorabile ascesa e gli indubbi vantaggi che questo nuovo paradigma porta con sé, ancora appare scarso, in Italia ma anche negli altri Paesi UE, il cosiddetto ***Big Data Analytics*** (BDA), ossia quell'insieme di processi utilizzati per l'analisi di queste enormi moli di dati, che è poi ciò che rende questi ultimi tanto preziosi per le imprese. Stando ai dati Eurostat, infatti, nel 2016 solo il 9% delle imprese italiane ha utilizzato strumenti di BDA, poco meno d'altra parte della media UE (10%).

Se i benefici sono oramai piuttosto chiari a chiunque, quello che richiede oggi l'attenzione e l'impegno da parte di tutti sono invece **gli aspetti critici e gli ostacoli** che, se non affrontati, rischiano di impedire la reale e piena realizzazione del potenziale dei Big Data.

I temi di maggior rilievo sono:

1) **la mancanza, attuale e futura, di competenze** critiche, atte a formare profili professionali specifici (quali data scientist, data architect ed esperti in Data Management), già ad oggi fortemente richiesti ma carenti sul mercato del lavoro: secondo le stime, il gap di competenze nel 2016 ammontava a circa 420.000 posizioni di *data worker* – il 6,2% della domanda totale – cifra che ci si aspetta salga entro il 2020 addirittura a 769.000, pari il 9,8% della richiesta di figure professionali. I Big Data non ridurrebbero dunque il contributo umano all'interno dei processi aziendali, ma piuttosto rivoluzionano i ruoli aziendali, dai manager ai lavoratori, creandone di nuovi;

2) **la carenza di investimenti in infrastrutture adeguate** a sostenere il nuovo paradigma tecnologico (reti veloci, 5G, infrastrutture di sicurezza);

3) **la garanzia della privacy e sicurezza del dato**;

4) **la proprietà del dato**, tema rispetto al quale si rende necessario un vero e proprio cambio di paradigma nel concetto di proprietà del dato personale, che ponga il singolo individuo al centro, restituendogli trasparenza e diritti, la cosiddetta democratizzazione dei Big Data;

5) **il c.d. *data divide***, ossia quel gap che va generandosi tra coloro che utilizzano ampiamente gli strumenti digitali e coloro che, facendo invece un uso molto marginale (se non nullo) di dispositivi digitali e producendo dunque una quantità di dati molto contenuta, rischiano di vedere le proprie esigenze, i propri valori e le proprie opinioni poco rappresentate.

Tra le sfide elencate, sicuramente, quella inerente alla necessità di competenze digitali superiori (o più avanzate) è la più sentita ed è stata sollevata anche durante il tavolo di discussione promosso da I-Com. In particolare, le competenze digitali di più alto profilo sono fondamentali per poter trarre valore dall'enorme mole di dati che, pur essendo a disposizione di tutti, necessitano di essere decifrati: per tale motivo sono opportune competenze e figure professionali specifiche (es. data scientist) e strumenti di intelligenza artificiale, quali apprendimento automatico o machine learning, che non solo sono in grado di raccogliere e ordinare i dati ma anche di analizzarli e trarre informazioni strutturate.

Tutti i partecipanti ritengono le competenze digitali – almeno quelle di base – un nodo fondamentale con conseguente necessità di investire in formazione, diffondere la cultura della digitalizzazione e promuovere l'alfabetizzazione informatica per far sì che tutti gli attori del sistema siano in grado di partecipare in modo attivo e consapevole ad una società sempre più digitalizzata.

Oltre alle competenze, per poter sfruttare e beneficiare del potenziale dei Big Data e in generale della rivoluzione digitale in atto è opportuno dotarsi di infrastrutture adeguate: soprattutto la pubblica amministrazione deve fare uno sforzo maggiore migliorando l'offerta dei servizi digitali e lavorando sull'interoperabilità. È, dunque, fondamentale creare un ecosistema collaborativo in cui vi siano sinergie e partnership tra soggetti pubblici e privati, che siano in grado di lavorare insieme per poter cogliere al meglio i benefici offerti dalle nuove tecnologie.

Relativamente all'aspetto della proprietà del dato, secondo alcuni dei partecipanti, sarebbe auspicabile l'introduzione di un registro universale dei consensi dove ciascuno possa liberamente dare o revocare il consenso al trattamento dei propri dati personali.

A fronte delle complesse sfide da affrontare soprattutto con riguardo alla tutela della sicurezza dei dati, l'Unione europea, il 27 aprile 2016, ha varato il **Regolamento 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati** con il quale è stata abrogata la direttiva 95/46/CE e che verrà immediatamente applicato, in tutti gli Stati membri, a partire dal 25 maggio 2018. Si tratta di un intervento normativo di grande rilevanza che ha fissato i fondamenti di liceità del trattamento dei dati, indicato in maniera tassativa tempi, contenuti e modalità dell'informativa, definito i diritti degli interessati (accesso, cancellazione-oblio, limitazione del trattamento, opposizione, portabilità), individuato le caratteristiche soggettive e le responsabilità di titolare e responsabile del trattamento (introducendo, tra i vari criteri, quello della "data protection by default and by design" e del rischio) e disciplinato i trasferimenti internazionali di dati.

I Big Data, uniti all'elevata e consolidata capacità computazionale, costituiscono i principali fattori abilitanti che spingeranno ancora di più il progresso dell'intelligenza artificiale, intesa come la scienza che si occupa di come creare sistemi informatici in grado di eseguire compiti che normalmente richiedono l'intelligenza umana.

L'**intelligenza artificiale** è stata sempre oggetto di interesse. La domanda «potrebbero essere in grado le macchine di pensare?» ha interessato tanto filosofi quanto scienziati e ingegneri e la prospettiva di riuscire a creare un giorno una macchina che possa imitare il comportamento umano è emersa in molti periodi storici. Oggi, si fa coincidere la nascita dell'intelligenza artificiale moderna con gli anni '50. Fu questo il periodo in cui ci fu la comparsa dei primi calcolatori elettronici e la pubblicazione dell'articolo di Alan Turing dal titolo "Computing machinery and intelligence", che fu considerato da molti il manifesto dell'intelligenza artificiale e nel quale fu introdotto il famoso test (cosiddetto "Test di Turing"), per determinare se e quando una macchina si possa considerare intelligente.

Da allora l'intelligenza artificiale ha fatto enormi passi in avanti e attualmente ci sono **molte applicazioni pratiche che riscuotono notevole interesse e stanno modificando alcune attività aziendali e il modo di interagire delle aziende con i consumatori**. Le più comuni sono: i **chatbot** - software di intelligenza artificiale che elaborano e interpretano il linguaggio naturale e, se opportunamente addestrati, dialogano con degli interlocutori umani allo scopo di fornire informazioni o compiere determinate operazioni; i **robot industriali**, che vengono utilizzati nelle attività di produzione e confezionamento merci o per l'assemblaggio e la saldatura di materiali. A questi spesso si associano anche i **cobot**, ovvero robot industriali collaborativi ideati per lavorare a stretto contatto con l'uomo. Altre applicazioni di intelligenza artificiale utilizzate nei più disparati settori economici (dalle TLC alla GDO, dal settore finanziario a quello sanitario) sono le tecniche di analisi dei dati, quali **Data Mining, Machine Learning, Deep Learning**, in grado di estrarre conoscenza da banche dati di grandi dimensioni tramite l'applicazione di algoritmi.

L'impatto disruptive delle nuove tecnologie riguarderà, dunque, diversi settori economici; sicuramente, l'high tech, l'automotive, il manifatturiero e i servizi finanziari sono e saranno i principali settori ad essere interessati ma gli effetti di questa nuova frontiera digitale interesseranno – e in parte già lo fanno – anche il settore del turismo, della sanità e dell'istruzione.

Relativamente al **settore finanziario**, le banche già da alcuni anni utilizzano strumenti di intelligenza artificiale, machine learning e deep learning. Semplici processi e/o attività, come l'apertura o chiusura dei conti correnti, vengono oggi affidati all'intelligenza artificiale con conseguente risparmio di tempo e possibilità di liberare risorse, che possono essere poi impiegate per attività commerciali di più alto profilo. Ciò che si ritiene fondamentale anche per gli esperti del settore finanziario seduti al tavolo I-Com è l'alfabetizzazione digitale e la consapevolezza dei rischi. È opportuno investire in campagne

di formazione e informazione e soprattutto assistere in maniera continuativa i clienti meno evoluti dal punto di vista digitale in modo tale da non lasciare nessuno indietro.

La digitalizzazione ridefinisce anche il **settore energia** (elettrico e gas), che pur essendo un po' in ritardo rispetto ad altri settori (soprattutto la parte gas) sta cercando di recuperare il gap, affiancando l'utilizzo di canali tradizionali (es. call center) a nuovi canali per gestire i rapporti con gli utenti/consumatori. Nello specifico, i big data e l'intelligenza artificiale porteranno ad un mutamento del rapporto tra aziende e consumatori. Si sta andando verso un sistema di co-creazione di offerte, che partendo dalle abitudini di consumo e intercettando i bisogni cerca di soddisfare al meglio le esigenze dei consumatori. In tale contesto, questi ultimi assumono un ruolo maggiormente attivo e diventano più consapevoli dei propri comportamenti. La consapevolezza del consumatore è il motore fondamentale e le aziende hanno il compito di spiegare i benefici delle nuove tecnologie e dare evidenza all'ampia platea di utenti di come i dati vengono utilizzati e gestiti, al fine di creare un clima di fiducia che agevoli la transizione verso una società sempre più informatizzata in grado di apportare numerosi vantaggi per entrambe le parti (impresa e consumatore). Ad esempio, nel settore energia, l'utilizzo delle nuove tecnologie consente di eliminare gli errori di fatturazione e quindi di ridurre le maxi bollette da conguaglio, nonostante sembri che, stando a quanto emerso dal tavolo di confronto, la bolletta 2.0 non abbia sinora portato risultati eclatanti, a dispetto dei diversi vantaggi ad essa generalmente associati, tra cui un risparmio di costi. Inoltre, l'utilizzo di motori semantici permette una risoluzione rapida delle controversie.

Al di là del rapporto con i consumatori, tema importante è anche la digitalizzazione delle reti. L'elettrificazione dei consumi (mobilità elettrica) pone la necessita di revisione e maggiori investimenti delle infrastrutture, che devono essere in grado di sostenere l'evoluzione in atto.

Contrariamente al settore energetico, il **settore idrico** si sta approcciando adesso alle dinamiche della rivoluzione digitale, lo stesso vale per il settore ambiente, dove si evidenzia una digitalizzazione a macchia di leopardo e differenze sostanziali tra le varie zone d'Italia.

Infine, nel settore energetico assume particolare importanza il **Sistema Informativo Integrato** gestito in maniera terza da Acquirente Unico, che nato come piattaforma digitale per lo scambio sicuro e affidabile di dati tra tutti gli operatori, sta diventando uno strumento fondamentale per agevolare lo sviluppo del mercato. È necessario però progredire sotto alcuni aspetti, quali: 1) accesso al cliente finale; 2) Cyber security; 3) Tutela della privacy; 4) collegamento ad altri database (ad es. Agenzia delle Entrate o Inps) per migliorare il servizio al cliente (es. erogazione bonus energia).

Per sopravvivere è necessario che le imprese siano in grado di assimilare tale cambiamento, avendo una visione olistica nel ripianificare il proprio business, ridisegnare i confini dello svolgimento delle proprie attività e ridefinire la catena del valore e le relazioni con partner e fornitori allo scopo di non farsi travolgere dalle innovazioni in arrivo, bensì coglierne le opportunità, che sembrano essere numerose. In particolare, l'intelligenza artificiale migliorerà l'attività di profilazione dei clienti e

personalizzazione del prodotto; l'apprendimento automatico (Machine Learning) permetterà alle aziende, ad esempio, di avere grafici previsionali in tempo record, schemi sui consumi della fase produttiva e suggerimenti per come migliorarne l'efficienza operativa. Inoltre, grazie all'intelligenza artificiale sarà più facile prevedere le spese e gli introiti su base mensile e annua e questo aiuterà a gestire al meglio il capitale aziendale da destinare agli investimenti. Infine, l'automazione e l'ausilio di robot industriali consentirà di eliminare mansioni ripetitive e pericolose.

Il consolidarsi dell'intelligenza artificiale ha spinto verso una crescita esponenziale del mercato mondiale. IDC stima che i ricavi mondiali derivanti dalle applicazioni di intelligenza artificiale e cognitive computing raggiungeranno circa 13 miliardi di dollari per fine 2017 ed entro il 2020 saranno superiori a 46 miliardi di dollari. In questo trend si inserisce anche il fenomeno della crescita del fatturato generato dalle chatbot e dell'incremento del numero di installazioni di robot industriali che, secondo i dati del World Robotics 2017, aumenteranno di almeno il 18% nel 2017 rispetto al 2016, raggiungendo le 346.800 unità per poi arrivare a circa 520.900 unità nel 2020.

L'intelligenza artificiale consentirà, dunque, lo sviluppo di grandi opportunità ma al contempo genererà profondi cambiamenti sulla società, ponendo sfide dal punto di vista operativo, etico ed economico. Pertanto è fondamentale superare gli ostacoli educativi ed emotivi legati alle soluzioni di intelligenza artificiale e creare un sistema che permetta, attraverso la trasparenza e la corretta informazione, di far capire le enormi **potenzialità dell'intelligenza artificiale** e che porti a scelte basate su consapevolezza e consenso, e che sia, inoltre, in grado di minimizzare le asimmetrie informative. In questo contesto un ruolo importante deve essere ricoperto dalle aziende in primis e anche dalle associazioni di consumatori, che devono non solo ampliare le proprie conoscenze e competenze ma anche informare ed educare correttamente i consumatori, soprattutto i più giovani che molto spesso sottovalutano i rischi legati alle nuove tecnologie. Infine, l'implementazione dell'IA deve essere accompagnata da una riflessione attenta su **privacy, sicurezza e protezione dei dati personali**.

Consapevoli delle potenzialità criticità connesse alla diffusione delle intelligenze artificiali - prima tra tutte, la tutela dei dati - **il Parlamento europeo, nel febbraio 2017, ha adottato una Risoluzione recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica**. In prospettiva de jure condendo il Parlamento ha formulato una serie di importanti proposte tra cui si segnala: 1) rafforzamento degli strumenti finanziari per i progetti di ricerca nella robotica e nelle TIC, compresi i partenariati pubblico-privati, e promozione di programmi di ricerca tesi ad analizzare i possibili rischi e le opportunità a lungo termine dell'intelligenza artificiale e delle tecnologie robotiche; 2) avvio di un dialogo pubblico strutturato sulle conseguenze dello sviluppo di tali tecnologie; 3) definizione di un quadro che soddisfi i requisiti di connettività per il futuro digitale dell'Unione e a garantire che l'accesso alla banda larga e alla rete 5G sia pienamente conforme al principio di neutralità della rete; 4) avvio di una riflessione sulla possibilità di istituire un'Agenzia europea per la

robotica e l'intelligenza artificiale; 5) valutazione delle implicazioni delle diverse soluzioni giuridiche tra cui: a) l'istituzione di un regime assicurativo obbligatorio; b) la costituzione di un fondo di risarcimento; c) la possibilità per il produttore, il programmatore, il proprietario o l'utente di beneficiare di una responsabilità limitata qualora costituiscano un fondo di risarcimento nonché qualora sottoscrivano congiuntamente un'assicurazione che garantisca un risarcimento in caso di danni arrecati da un robot; d) la scelta tra la creazione di un fondo generale per tutti i robot autonomi intelligenti o di un fondo individuale per ogni categoria di robot e tra il versamento di un contributo una tantum all'immissione sul mercato di un robot o versamenti regolari durante la vita del robot; e) l'istituzione di un numero d'immatricolazione individuale; f) l'istituzione di uno status giuridico specifico per i robot nel lungo termine.

La regolazione dovrebbe seguire l'evoluzione di questi strumenti tecnologici con regole non troppo stringenti e vigilare sulla corretta applicazione delle stesse.

I-GROUP 2 - Privacy e sicurezza nel cyberspace: quale tutela per consumatori e imprese?

L'evidente contesto di digitalizzazione degli utenti e delle imprese impone una riflessione sul **tema della sicurezza informatica** dal momento che le minacce e i crimini informatici stanno crescendo in misura esponenziale. Il 2016 è stato definito l'*annus horribilis* della sicurezza informatica avendo registrato il più alto numero di attacchi informatici degli ultimi tre anni. Il 72% del totale degli attacchi a livello mondiale ha riguardato i cyber crime, con la restante parte suddivisa tra hackeraggi, spionaggio e sabotaggio e guerra cibernetica. In particolare, la scena della sicurezza informatica degli ultimi tre anni è stata dominata dai **ransomware**, ovvero virus informatici che limitano l'accesso del dispositivo che infettano, richiedendo un riscatto da pagare per rimuovere la limitazione. Vittima principale degli attacchi informatici, principalmente dei ransomware, è stato il settore della sanità, che negli ultimi anni sta diventando il nuovo fronte caldo del crimine informatico, seguito dalla grande distribuzione organizzata e dal settore bancario/finanziario. Secondo gli analisti, i virus del riscatto tradizionale, che si sono abbattuti a pioggia sui computer di utenti, professionisti, imprese, appaiono rallentare come fenomeno. Ciò è probabilmente dovuto a più efficaci e diffuse strategie di backup dei dati; alla disponibilità di strumenti per decifrare alcune varianti del virus; ad alleanze tra soggetti pubblici e privati. Ma gli esperti ci mettono in guardia: i cybercriminali sono molto rapidi e flessibili nella loro capacità di adattamento e, infatti, starebbero già riposizionando i ransomware verso target di più alto profilo, verso vittime più vulnerabili e capaci di pagare di più. Altro **osservato speciale sul fronte della cybersicurezza è il mondo dell'Internet delle cose nei suoi vari ambiti applicativi**, in cui crescono potenzialmente le insidie e per tale motivo le aziende devono essere in allerta ed acquistare dispositivi aziendali che possano essere configurati e adattati coerentemente con le policy

di sicurezza. Tenendo conto delle future tendenze dei crimini informatici è, dunque fondamentale avere una visione strategica della sicurezza, competenze adeguate ed investire maggiori risorse.
A fronte di tale scenario, le esperienze personali dirette di abusi e violazioni dei dati personali e della privacy, dal 2010 al 2015, relativamente all'Italia, diminuiscono di 0,5 p.p, passando al 6% degli utenti internet, in linea rispetto al dato generale dell'Unione europea in calo di 0,6 p.p rispetto al periodo di riferimento, con l'ultimo dato al 3,4%. Inoltre, il 24,2% dichiara di essere stato vittima di un virus (un dato che, sebbene dimezzatosi nel corso dell'ultimo quinquennio, resta comunque superiore alla media europea). **Appare interessante notare come, in Italia ma anche – e ancor più marcatamente – nell'UE, la tendenza ad esser colpiti da un virus informatico sia più elevata tra i giovani**, i cosiddetti *digital native*, che dovrebbero essere più avvezzi all'uso degli strumenti digitali ed ai rischi che dietro di essi si nascondono: al contrario, invece, vuoi per un uso meno cauto del web e dunque una maggiore esposizione al rischio, vuoi per una minore consapevolezza dei rischi connessi, l'incidenza nella fascia d'età compresa tra i 16 e i 24 anni appare superiore al dato medio: 28,5% in Italia e 23,6% in UE. Siamo di fronte ad una situazione particolarmente complessa e pericolosa rispetto alla quale cresce l'attenzione delle imprese, sebbene appaiano anche segnali positivi: nel 2015, il 2,1% degli utenti Internet ha subito una perdita economica per frodi informatiche - un dato relativamente contenuto e comunque in contrazione rispetto al 2010 (-1,8 p.p.) - e solo circa un individuo su quattro (tra quelli che fanno uso regolare del web) appare preoccupato dei rischi informatici connessi ad un acquisto online, a fronte del 44,2% di solo cinque anni prima. **Sono** dunque **stati fatti, evidentemente, dei passi in avanti nel tempo, ma c'è sicuramente molto ancora da fare se, nell'era digitale, una fetta importante degli utenti Internet appare ancora molto preoccupata dell'aspetto sicurezza al punto tale da modificare i propri comportamenti in rete (o addirittura rinunciare ad entrare nel mercato digitale)**. In questo senso un ruolo importante lo giocano le imprese stesse, che affrontando il tema possono garantire una maggiore sicurezza ai propri clienti/utenti, ma anche a sè stesse, salvaguardando il corretto svolgimento delle proprie attività economiche. Sale, in effetti, il livello di allerta tra le imprese che, nel tempo, hanno risposto, in misura crescente, impiegando al proprio interno formali politiche di sicurezza sull'ICT. Al 2015, il 42,9% delle imprese italiane (29,4% nel 2010) risulta aver formalizzato una politica di sicurezza informatica, un dato nettamente superiore alla media europea (31,6%), ma ancora basso se si considera la portata del fenomeno. Va notato, tuttavia, che il problema vero risiede principalmente tra le PMI: in Italia, ad esempio, solo un'impresa su cinque non si è munita di una specifica politica interna di sicurezza informatica; tuttavia, meno di una PMI su due risulta esserne dotata (il 42% precisamente). La principale preoccupazione delle imprese è legata alla distruzione o corruzione di dati, rischio particolarmente sentito in Italia, dove il 37% delle imprese adotta una politica di protezione contro questo genere di rischio (quasi 10 p.p. in più rispetto alla media europea).

Relativamente a quanto emerso dal **tavolo di discussione promosso da I-Com**, **un esempio dei rischi quotidiani della rete sono le truffe dei pagamenti a seguito del furto d'identità**: il trafugamento dei dati di accesso ad una email personale non costituisce solo un vulnus alla privacy e al diritto alla segretezza della propria corrispondenza, ma può avere effetti economici significativi in danno deii soggetti coinvolti. La Polizia Postale ha segnalato la diffusione di truffe economiche in rete del tipo "man in the middle", cioè operazioni di pagamento tra due soggetti, uno dei quali subisce un furto di identità da parte di un cyber criminale che intercetta, dunque, il relativo pagamento e compie la truffa.

Probabilmente si porrà, in chiave evolutiva, il tema della allocazione della responsabilità civile in capo all'impresa che, non avendo adottato efficaci sistemi di sicurezza, è stata vittima di un attacco informatico le cui conseguenze pregiudizievoli siano transitate sui consumatori o su altri soggetti che intrattenevano rapporti commerciali con l'impresa in questione.

È stato poi sottolineato, anche in questa sede, come **la consapevolezza dei cittadini e delle imprese** sia **un'arma indispensabile per contrastare i rischi legati al mondo digitale**. Infatti, la consapevolezza rimane al primo posto tra gli obiettivi degli operatori della sicurezza, siano questi istituzionali o privati. Dal Governo alle associazioni dei consumatori sono tutti impegnati nel sostenere i processi di informazione ed "educazione digitale", con l'obiettivo di creare quella che, quasi come un ossimoro, viene definita "**cybersecurity domestica**". A tali processi va, inoltre, associata una **specifica formazione scolastica**, coinvolgendo i "nativi digitali", non solo perché sono i soggetti maggiormente esposti, ma anche perché, al fine di creare un'autentica cultura della sicurezza, occorre che la presa di coscienza della dimensione digitale in tutte le sue forme e in tutti i suoi potenziali rischi sia un elemento che accompagna l'individuo sin dal primo approccio con le nuove tecnologie. **La cybersecurity e la relativa consapevolezza, tuttavia, non devono interessare solo la dimensione domestica e scolastica, ma contestualmente devono avvolgere la sfera del mondo del lavoro.**

Come detto poc'anzi, **la sicurezza informatica è entrata a pieno titolo nel tema della sicurezza nazionale**. Pericoli che riescono a coinvolgere, senza difficoltà alcuna, dal singolo individuo connesso dalla propria abitazione – dalla comune navigazione su Internet, sino alla violazione degli arredamenti ed elettrodomestici smart, parte dell'ecosistema dell'IoT – alle infrastrutture critiche nazionali. Esemplare è l'intrusione di Anonymous – la famosa organizzazione internazionale di hacker – all'interno dei sistemi di diverse Istituzioni italiane che ha avuto come effetto la pubblicazione di alcuni documenti riservati in Rete. In questo contesto, oltre alle risposte dei privati – come il sempre più numeroso gruppo di imprese dotate di politica di sicurezza ICT – anche le Istituzioni, a tutela dell'ordine pubblico e delle strutture strategiche, hanno prodotto risposte legislative che mirano ad efficientare il comparto della sicurezza informatica, partendo da riforme strutturali – come è il caso dell'Italia – sino alla **creazione di una nuova Agenzia per la Cybersecurity e di una comune**

certificazione – come previsto dalla Commissione Europea e dalla relativa **proposta di regolamento presentata, durante il discorso del Presidente Juncker, allo Stato dell'Unione dello scorso 13 settembre**[1].

La Commissione ha deciso di tracciare una **roadmap da qui al 2020**, con l'obiettivo di migliorare la resilienza dei sistemi, la deterrenza e la difesa dagli attacchi cibernetici, grazie alla costruzione di una politica comune sulla cybersecurity, che prevede un piano di investimenti di 2 miliardi di euro entro il 2020 a cui fa seguito l'intero impianto applicativo, basato su 4 punti cardine: collaborazione tra gli Stati membri, ricerca costante, tempestivo controllo e risposte adeguate. Per consentire un maggior controllo e un efficientamento dei sistemi di sicurezza, la Commissione intende rafforzare il ruolo dell'ENISA (Agenzia Europea per la Sicurezza delle Informazioni e delle Reti), potenziandone il mandato, con più poteri e a tempo indeterminato ponendola al centro della politica comune di difesa e affiancandola agli Stati membri nella lotta al crimine informatico.

Maggior sicurezza informatica significa anche univocità riguardo ai sistemi di certificazione che attestano la sicurezza dei sistemi. Purtroppo, all'interno del territorio comunitario, esistono diverse tipologie di certificazione con standard differenti e tale diversificazione rende gli stessi, in particolare quelli sviluppati su base nazionale, deboli e addirittura inutilizzabili nel Mercato Unico. Per far fronte a tale esigenza, la Commissione, grazie anche al lavoro dell'Agenzia, intende porre in essere degli standard comuni di sicurezza informatica, adducendo l'intero Mercato Unico nel riconoscimento ex omnibus partibus di una certificazione di cybersecurity, producendo due effetti immediati, uno di tipo economico e l'altro di tipo qualitativo. Sul piano qualitativo, l'intento dell'UE è di assicurare che tutti gli organi di certificazione verifichino il rispetto dei livelli minimi di sicurezza approvati dalle stesse Istituzioni europee. Una parificazione normativa che innalzerà i livelli di cybersecurity in quegli Stati membri ancora poco in linea con altri Paesi più avanzati sul comparto. Più chiarezza e univocità a favore dei consumatori che potranno ottenere un unico punto di riferimento sugli acquisti dei prodotti e dei servizi. In termini economici l'impatto sarà positivo soprattutto per i produttori: ad oggi, sistemi di certificazione diversificati comportano molteplici richieste ad altrettanto molteplici enti certificatori, per i singoli Paesi membri, causando, alcune volte, disparità e disagio.

Anche l'Italia sta provando a fare la sua parte, con un proprio **Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica (PN)**, presentato lo scorso marzo, il quale si inserisce all'interno del più ampio Quadro Strategico Nazionale (QSN). Uno sviluppo di punti cardine per incrementare l'efficienza e la funzionalità della struttura di cybersecurity dello Stato. Centrale, per il PN, risulta essere la revisione del Nucleo per la Sicurezza Cibernetica, una contrazione della catena di comando per la gestione delle crisi cibernetiche e, quindi, la semplificazione dell'architettura nazionale, grazie alla soppressione o all'accorpamento di alcuni organi, tra i quali i CERT. **Un ruolo**

[1] *Factsheet on the EU Cybersecurity Agency*, EU Commission, 2017

chiave, riguardo la struttura nazionale di cybersecurity, l'avrà il DIS, soprattutto riguardo il coordinamento del nucleo operativo. Ruolo rilevante anche all'AgID, chiamata a indirizzare, assicurare e monitorare il rispetto degli standard nei sistemi informativi pubblici e relative reti di interconnessione. Oltre ad aspetti di tipo organizzativo, **il PN prevede un forte sostegno e impulso al mondo accademico, della ricerca e dell'imprenditoria con iniziative mirate: la creazione di una fondazione che abbia tale compito, il finanziamento di start-up del settore e la partecipazione al capitale societario di realtà imprenditoriali d'interesse, la realizzazione di un Centro nazionale di R&S sulla cybersecurity e uno sulla crittografia**. Il nostro Paese, attraverso questo Piano, intende rispondere alle esigenze emerse dal proprio tessuto sociale. Esigenze fattesi più stringenti a seguito del sempre maggior rischio a cui si è esposti, soprattutto tra le imprese.

Gli strumenti a disposizione per il contrasto delle attività criminose esistono, come abbiamo visto ma, senza ombra di dubbio, queste dovranno aumentare nella disponibilità e nella qualità, cercando di evolversi di pari passo, se non anticipandole, con le tecniche criminose utilizzate nell'ambito cyber. **Le istituzioni impegnate in prima linea su questo fronte hanno un ruolo chiave nell'implementare i sistemi di sicurezza, tuttavia, queste non possono essere sufficienti se inserite in un contesto prettamente nazionale. Il fenomeno degli attacchi informatici e della relativa cybersecurity**, a fronte della propria natura cross-border tra gli Stati, **non può che esigere risposte di tipo sovranazionale,** possano essere provenire dall'Unione Europea e/o frutto di accordi internazionali.