CAPITOLO 3

Tutela della privacy

La protezione dei dati personali diventa «responsabilità»

di **Aldo Bottini**

L'entrata in vigore del regolamento europeo in materia di protezione dei dati personali (Gdpr), alla quale mancano ormai pochi mesi, è una questione di grandi dimensioni; grande è la portata della norma (europea, certo, e addirittura più ampia), grandi i rischi per i trasgressori (si è parlato spesso e si parlerà ancora delle sanzioni e della loro misura), grande il cambio di passo che ha portato la privacy in pochi anni (se non in pochi mesi) sulle prime pagine dei giornali e nei verbali di e nelle stime di consigli di amministrazione e revisori contabili.

Compresa quindi l'importanza della riforma, quale impatto avrà, il Gdpr, sulla quotidianità delle aziende? Per rispondere a queste domande è necessario partire da una delle novità più rilevanti del Gdpr rispetto al nostro Codice della privacy: si passerà da un sistema di misure minime di sicurezza per il trattamento dei dati (soddisfatti determinati parametri, il trattamento è legittimo) a un sistema di responsabilità del titolare per la sicurezza del dato trattato. In breve: il rispetto della privacy diventa un requisito necessario e mutevole (a seconda del dato, a seconda dei tempi, a seconda dello sviluppo tecnologico) di ogni trattamento.

Poiché sono i dipendenti a trattare i dati e poiché ogni società tratta i dati dei propri dipendenti, la prima fondamentale novità da mettere in conto è la formazione. Dopo aver adeguato i propri sistemi e i propri processi alle novità del Gdpr, ogni datore di lavoro dovrà formare i propri dipendenti, e chi li gestisce e controlla, al rispetto della normativa privacy. La formazione comprende: l'adozione di un preciso organigramma, la definizione dei ruoli, l'adozione di procedure in caso di data breach o emergenza.

Dal maggio del 2018, ogni dipendente dovrà sapere quale è il suo ruolo rispetto alla privacy e, corrispettivamente, come i suoi dati sono trattati nell'esecuzione del rapporto di lavoro. Non è necessaria una due diligence per affermare che la funzione di gestione delle risorse umane tratta dati (spesso sensibili) in modo continuativo e tale trattamento dovrà avvenire secondo i nuovi principi di responsabilità introdotti dal Regolamento. A ciò si aggiunga che l'eventuale nomina di un Dpo aggiunge una figura alla vita quotidiana di ogni azienda, con la parallela esigenza, per realtà di dimensioni importanti, di strutturare un ufficio che vigili e gestisca gli aspetti privacy dell'attività. Se, infatti, non è obbligatorio, avere un ufficio privacy interno, può essere la soluzione più semplice all'esigenza di chiarezza e accountability disegnate dal Gdpr. Nel nuovo sistema, occorrerà infatti dimostrare di avere messo in campo a priori ogni cautela per la gestione dei dati.

Il Gdpr aumenterà rischi e sanzioni per chi sbaglia Aziende obbligate a formare i dipendenti

NUOVA PRIVACY, siamo **IN RITARDO**

MAG ne ha parlato con Maria Roberta Perugini, partner di Jacobacci. «Norme sottovalutate». Ecco come si dovrà procedere per adeguarsi. E gli studi legali non faranno eccezione

Il 25 maggio diventerà applicabile la nuova privacy europea. La sensazione però è che in Italia si sia già tutti in ritardo. In effetti, nel corso dell'anno e mezzo trascorso dall'entrata in vigore del GDPR, diversi organismi hanno effettuato ricerche per analizzare il livello di consapevolezza delle imprese e di attivazione per l'adeguamento. I risultati sono sempre coerenti nell'evidenziare che, ancora oggi, più della metà degli operatori (soprattutto se Pmi) non ha reale consapevolezza dell'impatto della nuova normativa e non ha avviato azioni per adeguarsi. Purtroppo si tratta di un problema rilevante. La nuova privacy è un tassello (insieme ad altri, ad esempio le misure per lo sviluppo delle infrastrutture digitali e quelle per l'incentivazione del commercio elettronico transfrontaliero) di un progetto molto più ampio per la creazione di un mercato unico digitale che la Ue ha definito, condiviso e perseguito sin dal 2015.

«Dobbiamo considerare la *compliance privacy* come uno strumento essenziale per sostenere e incentivare i nuovi modelli di sviluppo economico fondati sull'innovazione», dice in questa intervista **Maria Roberta Perugini**, partner di Jacobacci. «La trasformazione digitale crea nuovi mercati di sbocco e l'ampliamento di quelli tradizionali. Crea nuovi prodotti e servizi, nuovi processi di produzione e vendita, nuove relazioni nel mondo del lavoro».

La Ue, nella sua comunicazione di maggio scorso sulla revisione intermedia della strategia per il mercato unico digitale, ha sottolineato come il rispetto della vita privata e la protezione dei dati personali siano due condizioni che garantiscono la fiducia dei consumatori verso l'impresa e di conseguenza la stabilità, la sicurezza e la competitività dei flussi commerciali mondiali. «Le imprese che non riusciranno a realizzare la transizione sono inesorabilmente destinate a restare indietro», sottolinea l'avvocata.

Il GDPR va visto in questo contesto e ognuno deve fare la sua parte, compresi i legislatori nazionali, che hanno la responsabilità fondamentale di compiere interventi tempestivi sul quadro legislativo nazionale in un'ottica di armonizzazione con la normativa europea.
La legge di delega al Governo per adeguare il quadro normativo nazionale alle disposizioni del Regolamento è di ottobre scorso (quindi, già in grande ritardo sulla tabella di marcia) e prevede un termine di ulteriori sei mesi per l'emanazione di appositi decreti: in pratica, fino all'inizio di maggio.

«Un adeguamento **"standard"** è perfettamente **inutile**, a prescindere dai costi sostenuti per attuarlo. Il **25 maggio** è solo il **punto zero** di un percorso che **comincia** e che **continua** finché l'impresa opera trattamenti»

In attesa dei decreti delegati, però, alcune nuove disposizioni in materia sono state inserite nella legge europea 2017 e poi nella legge di Bilancio 2018, mentre un ulteriore specifico provvedimento a fine anno ha modificato la disciplina del registro delle opposizioni e dunque del telemarketing...
Sì, ma queste innovazioni, in parte perché sono intervenute su temi molto specifici e in parte per il contenuto perlomeno opinabile, certamente non stanno contribuendo a dare chiarezza e organicità al quadro normativo in materia e anzi – in alcuni casi – sembrano addirittura contrastare con specifiche norme del GDPR.

Che atteggiamento riscontra tra imprese e soggetti interessati?
Purtroppo, nella mia esperienza professionale constato che moltissime realtà imprenditoriali sono ancora oggi ignare del ruolo fondamentale giocato nello sviluppo economico dalle norme a protezione dei dati personali. Queste, anzi, assai spesso vengono sottovalutate, affrontate con un approccio formalistico e interpretate (con fastidio) come richiesta di adempimenti amministrativi aggiuntivi, privi di rilevanza sostanziale.

Bene, allora da cosa bisogna cominciare?
Dal convincersi che la soluzione è sviluppare una reale capacità di *data governance*. Moltissime organizzazioni non hanno consapevolezza effettiva della mole dei dati che trattano e delle loro caratteristiche, e neppure

sanno con esattezza dove sono archiviati e da chi e come sono utilizzati... È chiaro che in queste condizioni non solo non è possibile alcuna efficace gestione del rischio di *data breach*, ma neppure vi sono i presupposti per effettuare quel salto di qualità nella gestione delle informazioni aziendali.

E quindi?
La prima cosa da fare dunque è un'analisi approfondita dell'azienda. I risultati di questa analisi sono la base per verificare il livello di conformità effettivo dell'ente al GDPR e per individuare le azioni da assumere al fine di raggiungere una conformità piena (*gap analysis*), e ciò sia sotto il profilo della sicurezza sia sotto quello documentale e organizzativo.

E a questo punto?
Una volta individuati i propri obiettivi di *accountability*, l'impresa deve definire un primo piano per soddisfarli. A conclusione di questi passaggi, l'impresa sarà in grado di produrre il proprio modello di gestione privacy. A questo punto – e solo a questo punto – dovranno e potranno essere operate le azioni concrete volte all'attuazione degli specifici interventi individuati, diretti alla implementazione del modello di gestione privacy aziendale.

Esiste un modello valido per tutti?
Un adeguamento "standard" è perfettamente inutile, a prescindere dai costi sostenuti per attuarlo. Il 25 maggio è solo il punto zero di un percorso che comincia e che continua finché l'impresa opera trattamenti. È importante la partecipazione attiva dell'ente alla progettazione e attuazione di un percorso personale di conformità, anche condotto con il supporto di consulenti esperti, costituisce l'ottimale strumento per giungere a gestire in autonomia la compliance nel continuo.

Adeguarsi sarà costoso? E quanto?
Certamente, operare per la compliance comporta dei costi. Ma è l'unico strumento per mitigare il rischio di sanzioni che con il GDPR possono arrivare fino a 20 milioni di euro o – se superiore – al 4% del fatturato mondiale annuo di gruppo.

Chi è il Dpo? Cosa fa?
Possiamo dire che il Dpo è una "misura di sicurezza": questa figura è esplicitamente prevista e regolamentata dal GDPR. È uno strumento fondamentale dell'*accountability*, il "direttore d'orchestra" del sistema di trattamento aziendale.

«A mio parere è necessaria una **competenza multidisciplinare**, che però ad oggi è estremamente **difficile da trovare** in una sola persona: credo che per il momento si affermerà maggiormente la scelta di costituire un *team*, magari guidato da un legale con **esperienza** in materia di *privacy* ma che comunque annoveri anche altri componenti, perlomeno con competenze informatiche, di ***cybersecurity*** e di ***governance*** **aziendale**.»

Lo deve fare l'avvocato? Il general counsel? Un tecnico?
Può essere un individuo o un team, così come in house o esterno, nominato sulla base di un contratto di servizi. La mia impressione è che, per il ruolo chiave che assume nell'ottica della conformità dell'ente, le realtà più complesse, non possano prescindere dall'avere un Dpo dedicato, e pertanto interno.

Con quali competenze?
A mio parere è necessaria una competenza multidisciplinare, che però ad oggi è estremamente difficile da trovare in una sola persona: credo che per il momento si affermerà maggiormente la scelta di costituire un team, magari guidato da un legale con esperienza in materia di privacy ma che comunque annoveri anche altri componenti, perlomeno con competenze informatiche, di cybersecurity e di governance aziendale.

Anche gli studi legali dovranno provvedere?
Gli studi legali operano trattamenti di dati personali come e più degli altri enti: certamente devono adeguarsi alla nuova normativa e ritengo che abbiano particolare interesse a farlo, visto che custodiscono le informazioni più preziose e riservate dei loro clienti. Anche tra gli studi legali vige la stessa regola delle imprese: chi ha consapevolezza dei rischi e delle opportunità legati all'innovazione, considera l'adeguamento al GDPR una priorità e un'opportunità; chi al contrario non ne è consapevole, si gira dall'altra parte o si limita a un adeguamento formale.

E sono pronti, gli studi?
Bisogna capire innanzitutto che la sicurezza non è solo un tema di *cybersecurity*, che pure è un aspetto essenziale: la sicurezza, prima ancora che dalla tecnologia, passa attraverso la conoscenza e il controllo dei propri processi di trattamento. È inutile avere a disposizione sofisticati firewall quando si consente ai collaboratori di utilizzare il proprio pc personale per accedere ai server, di navigare con device personali sulla wifi di studio senza un'adeguata configurazione degli accessi o di collegare al pc di studio hard disk esterni non autorizzati.

Per i consulenti sarà un buon filone di business. Ma per svolgere un'adeguata attività serviranno competenze multidisciplinari o è un lavoro solo per avvocati?
Un servizio di consulenza efficace in questo campo deve sapere collegare aspetti legali e possibili soluzioni tecniche e organizzative, per mettere l'azienda in grado di identificare gli interventi necessari assegnando le relative responsabilità, pianificare e ottimizzare gli interventi. È ovvio che per tutto questo sia necessario un approccio multidisciplinare (legale, governance, tecnico, organizzativo) e olistico che è nuovo con riferimento alla compliance privacy ma che non è esattamente assimilabile neppure alle attività di adeguamento ad altre normative.

Insomma, l'avvocato da solo non basta più?
Non basta più, così come il tecnico informatico, anche se esperto di cybersecurity, e l'esperto di governance aziendale: tutti però sono elementi essenziali e la stretta collaborazione tra di essi e i referenti aziendali, che sono i veri attori del trattamento, è la chiave per una consulenza di successo. ■

GESTIRE L'IMPRESA

Chi pensa che i dati siano il "nuovo petrolio" farà meglio a estendere il parallelo. Come per il petrolio, anche per usare i dati occorrerà dotarsi di costosissime licenze di sfruttamento. E sarebbe davvero ora di porre fine al saccheggio della nostra privacy in atto da anni. Lo impone, in Europa, la nuova direttiva Gdpr, in vigore da maggio. Ecco come adeguarsi.

30-34
EXPORT & IMPRESE
I NUMERI DELLA LOMBARDIA, IL MERCATO USA, I BILANCI

40
FEDERMANAGER
PREVIDENZA: «FATTI E NON DEMAGOGIA»

42
COST-MANAGEMENT
CON LA PREVENZIONE SI RIDUCONO I "PICCHI"

PRIVACY, PARTE IL COUNTDOWN E A FARE GLI STRUZZI SI RISCHIA

Tra tre mesi esatti entrerà in vigore il nuovo Regolamento europeo sulla tutela dei dati personali (Gdpr). E per le aziende che non si mettono in regola sanzioni fino a 20 milioni e il 4% del fatturato

di Marco Scotti

C'è un'enorme mucca nel corridoio e molti fanno finta di non vederla: l'entrata in vigore del Regolamento europeo sulla protezione della privacy (il General Data Protection Regulation meglio conosciuto come "GDPR",) è un fattore che cambierà radicalmente le carte in tavola per le aziende, anche quelle di piccole dimensioni. Dal 25 maggio prossimo, infatti, diventeranno obbligatori una serie di accorgimenti che tuteleranno le imprese in caso del cosiddetto "data breach", ovvero l'intrusione esterna con intenti predatori – in particolare per quanto riguarda il furto d'identità che, secondo una recente indagine di Microsoft, è l'obiettivo principale del 76% dei cyberattacchi. L'Italia non è messa benissimo. Prima di tutto perché è quarta al mondo per numero di incidenti informatici. Nel 2016 sono aumentati i tentativi di intromissione contro il Sistema Sanitario Nazionale del 102%, del 70% verso il settore retail e GDO, del 64% contro bank&finance. Questa attività criminale costa alle aziende italiane circa 900 milioni di euro. Ma – parafrasando un celebre slogan – "il peggio deve ancora venire". In caso di data breach, l'azienda avrà 72 ore di tempo per denunciare – dal momento in cui si accorge dell'intromissione – alle autorità competenti quanto accaduto. E se non lo fanno? Non conviene dire, un po' furbescamente, non ci siamo accorti di nulla? «No, perché si rischiano sanzioni fino a 10 milioni di euro in base ad alcune norme e per fino a 20 in base ad altro. Anche perché in primo luogo sono gli utenti ad accorgersi dell'intromissione, in nove casi su dieci. Ma anche se questo non dovesse accadere, sarebbe piuttosto semplice sostenere che, qualora dovesse emergesse ex post, che c'è stata data breach, la mancanza di detection

IN CASO DI INTROMISSIONE L'AZIENDA HA 72 ORE DI TEMPO PER COMUNICARLO ALLE AUTORITÀ COMPETENTI. E CHI NON LO FA RISCHIA MULTE SALATISSIME

Luca Bolognini, presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati, socio fondatore dello studio ICT Legal Consulting

rappresenterebbe essa stessa l'inadeguatezza delle misure di sicurezza, esponendo l'azienda a multe pesantissime». È questa la convinzione di Luca Bolognini, presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati e socio fondatore dello studio ICT Legal Consulting. Inoltre, le aziende che non siano compliant rispetto al GDPR rischiano una sanzione che può arrivare fino al 4% del fatturato globale, simile a quelle elevate dall'Antitrust.

Come sono messe le aziende? E la pubblica amministrazione? Bolognini non ha dubbi: «Da un lato sono fiducioso per quanto riguarda le grandi aziende che stanno galoppando e si stanno impegnando molto con i programmi di adeguamento. Mi preoccupano terribilmente gli enti pubblici perché adeguarsi significa investire fondi, risorse che la macchina pubblica difficilmente si può permettere e non sto parlando soltanto dell'adeguamento giuridico. Da quel punto di vista sono parecchio preoccupato. Anche perché il comune o l'ente locale viene sanzionato per la violazione di alcune norme fino a 10 milioni di euro e per altre fino a 20. E c'è l'articolo 80 che introduce una sorta di class action e quindi i comuni, che sono molto esposti, potrebbero trovarsi di fronte ad associazioni che saranno promotori dei controlli. Tutti gli enti pubblici che sono molto esposti verso i cittadini rischiano grosso».

Diventerà obbligatorio mettere in atto almeno tre soluzioni che, se combinate, garantiscono all'azienda di essersi comportata in maniera congrua alla nuova norma. Prima di tutto, i dati dovranno essere protetti da una password di almeno otto caratteri. In secondo luogo, bisogna separare il dato dall'identificativo in due luoghi diversi del server. Il terzo punto è quello relativo è all'anonimizzazione, che consente di eliminare qualsiasi riferimento alla persona, pur mantenendo i suoi dati. Inoltre, le aziende dovranno dotarsi nel loro organico di un DPO (Data Protection Officer), un esperto in diritto dei dati con competenza informatica, che dovrà essere assunto o che potrà collaborare esternamente. In entrambi i casi, il suo parere sarà vincolante per l'azienda. Qualche mese fa, proprio dalle colonne di Economy, avevamo stimato la necessità di circa 41 mila nuove figure professionali. Oggi queste stime rischiano di dover essere riviste al rialzo. «Non stiamo parlando del singolo medico che tratta dati o del singolo avvocato – ci ha spiegato Bolognini – ma anche di piccole o medie aziende nei quali vengono toccate informazioni sensibili. E, in ogni caso, sembra sempre più prudente avere un DPO in organico. Anche gestire le newsletter può diventare un tema sensibile, soprattutto perché chiunque utilizza questo strumento fa anche tracking online, utilizzando software che sono in grado di dire chi ha aperto la mail, se ha cliccato sui diversi

Occhio anche alle email, vanno seguite quattro regole d'oro

Consenso, informativa, privacy by design e diritto all'oblio sono i capisaldi su cui è costruito l'impianto del GDPR

di Alessio Beltrami

L'obiettivo del GDPR è chiaro in ogni sua riga: rimettere nelle mani del cittadino europeo un controllo totale dei propri dati, semplificando tutti quei processi che lo vedono protagonista sia nel consenso iniziale del trattamento dei propri dati, sia nella revoca. Il nostro indirizzo email è tra questi dati e il modo in cui le aziende gestiscono le nostre email è oggetto del nuovo regolamento. Va detto che nonostante l'abbondanza di nuovi strumenti digitali per comunicare con i clienti, l'email si dimostra essere ancora una delle scelte più intelligenti per mantenere relazioni commerciali. A conti fatti è lo strumento ideale per creare e consolidare un rapporto di fiducia tra azienda e cliente. Esistono però alcune condizioni da rispettare per fare sì che questo accada: benvenuti nella Data Economy dove sono i dati la vera moneta di scambio e come ogni moneta va tutelata. Ecco perché nei suoi punti non ci sono semplici disposizioni, ma un'esortazione continua a comunicare in modo semplice e trasparente aiutando l'utente a comprendere, in modo che l'argomento della privacy venga compreso e rispettato e non trattato come un semplice aspetto burocratico a cui adempiere perché obbligatorio. Per molto tempo la comunicazione via email è stata trattata con superficialità da parte delle aziende e questo non solo dal punto di vista norma-

link o se ha preferito cestinare la mail».

Ma è una legge che nasce già vecchia

Ma perché una nuova legge sulla privacy? Non era sufficiente l'impianto giuridico già esistente? «Prima di tutto per far prendere la privacy un po' più sul serio – puntualizza il presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati – le sanzioni non erano adeguate, erano molto basse e non venivano considerate un problema dalle grandi aziende. Oggi invece il tema viene imposto nell'ordine del giorno anche dei grandi board, che non possono più fare finta di niente. Inoltre, questo è un regolamento che prende in considerazione in maniera più adeguata tutte le problematiche comportate dall'era del digitale. Profilazione e algoritmi, in particolare, sono oggetto di un'attenzione maggiore. Infine, si tratta di un regolamento che si applica in maniera molto più forte anche a soggetti che operano al di fuori dell'Ue: venendo meno i confini continentali, anche nel trattamenti dei dati bisognava introdurre uno strumento che fosse più efficace». Piuttosto, quello che balza all'occhio è che si tratta di un regolamento che potrebbe diventare vecchio in breve tempo. Perché non tiene conto delle nuove frontiere della tecnologia e soprattutto delle novità nel campo dell'Information Technology. «Mi rendo conto che si rischi di andare su un versante un po' d'avanguardia – ha concluso Bolognini – ma questo è un regolamento che non prende in considerazione a sufficienza l'Internet of Things e l'intelligenza artificiale. È un regolamento che introduce soltanto il tema della responsabilità e dell'affidabilità, ma si tratta di una responsabilizzazione dei soggetti e degli esseri umani, mentre non si parla dell'accountability degli oggetti e dei robot. Eppure, in futuro sarà sempre più reale il fatto che i robot dialoghino tra loro scambiandosi informazioni anche sensibili senza controllo umano. Da questo punto di vista, il GDPR nasce abbastanza vecchio».

IL GDPR NON TIENE CONTO DELLE NUOVE FRONTIERE DELLA TECNOLOGIA E AFFIDA LA RESPONSABILITÀ SOLO ALLE PERSONE, NON ALLE MACCHINE

+102% AUMENTO CYBERCRIMINE CONTRO SSN

SANZIONE MASSIMA 4% FATTURATO GLOBALE

72 ORE DI TEMPO PER DENUNCIARE UN'INTRUSIONE

DPO NECESSARI IN ITALIA OLTRE 41MILA

900 MILIONI COSTO ANNUO PER LE AZIENDE

25 MAGGIO ENTRATA IN VIGORE NUOVO GDPR

tivo, ma anche dal punto di vista strategico. Se così non fosse, non conosceremmo la sensazione di ricevere quotidianamente email che provengono da mittenti a cui non abbiamo mai dato la nostra autorizzazione e inerenti a tematiche che nulla hanno a che fare con i nostri bisogni e interessi. Ecco i punti salienti:

1 CONSENSO INEQUIVOCABILE

Possono esserci diversi modi per ottenere il consenso al trattamento dei dati: per il GDPR, l'utente dovrà comprendere chiaramente di esprimere il suo consenso. Ecco perché la scelta non può essere espressa insieme ad altri consensi.

2 INFORMATIVA

Il contenuto dell'informativa diventa il protagonista e il GDPR impone testi semplici e comprensibili. L'obiettivo è far capire all'utente cosa succederà e come verranno trattati i suoi dati.

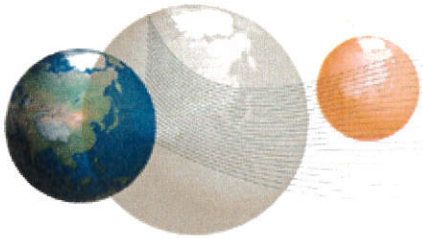
3 PRIVACY BY DESIGN

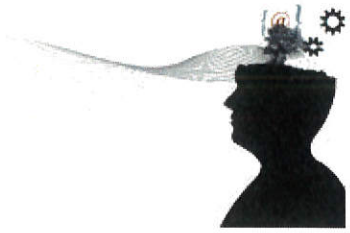
Nel GDPR emerge il concetto di Privacy by Design che potremmo riassumere così: smetterla di considerare la privacy come uno dei tanti adempimenti formali e burocratici e iniziare a considerarla come una vera priorità quando costruiamo azioni di raccolta ed elaborazione dati.

4 DIRITTO ALL'OBLIO

Con il diritto all'oblio l'utente avrà il diritto di richiedere la completa cancellazione dei dati che lo riguardano facendone sparire ogni traccia dai nostri database. Questo è un concetto più radicale del diritto alla cancellazione o dell'opposizione al trattamento (tutele attualmente in vigore) e richiederà alle aziende di organizzarsi per garantire l'effettiva cancellazione di ogni dato che riguardi l'utente.

*di Stefano Cuzzilla**





Il Gdpr è una questione manageriale

Più della metà delle aziende italiane spende meno del 3% del proprio *budget* ICT in sicurezza informatica. Da come si stanno muovendo le nostre imprese, c'è da ritenere che la protezione dei dati nell'era digitale appartenga al novero di quei problemi di cui ci si preoccupa solo quando è troppo tardi.
Dobbiamo lavorare, quindi, per far crescere l'attenzione che grandi aziende e soggetti pubblici stanno rivolgendo a soluzioni più integrate, sperando generi un effetto traino sulle realtà di dimensioni piccole e micro.
Mancano infatti appena sei mesi al momento in cui il Gdpr, il regolamento europeo 2016/679 che ha innovato profondamente la materia della *data protection*, diventerà vincolante in precetti e sanzioni.
Ci troviamo di fronte a una rivoluzione normativa che recepisce un cambiamento reale ineluttabile: la digitalizzazione delle attività e l'impulso della tecnologia applicata all'industria stanno capovolgendo tutto, trasformando la protezione del dato in un tema di massima urgenza.
Ecco perché è essenziale farci trovare preparati, consapevoli dell'impatto che la *data protection* produce sull'organizzazione aziendale e sulla competitività d'impresa. Non si sottolinea abbastanza, infatti, che questo è un tema che coinvolge tutto il *management* aziendale e non solo chi ha la responsabilità dell'IT.
Sono d'accordo con il garante europeo per la privacy, Giovanni Buttarelli, quando afferma che la gestione dei dati personali richiede un approccio diverso soprattutto da parte del *management*, con scelte strategiche e risorse dedicate. Ed è giusto anche – come ha sottolineato di recente – condividerne l'onere, perché si tratta di mettere in campo un gioco di squadra, in cui l'azione di tutti i soggetti presenti in azienda deve essere responsabilizzata. Altrimenti, il rischio è di impoverire la carica innovativa che il Regolamento europeo possiede, riducendolo a mero adempimento formale, a materia burocratizzata o, peggio, banalizzata.
Per questo, la figura del *data protection officer* che è prevista dal Gdpr deve qualificarsi con un profilo manageriale: non basta affidarsi a un *hardware* di competenze tecniche in grado di prevenire e poi operare nel *crisis management*. Servono *manager* con *soft skill* adeguate per trasferire la cultura del rischio informatico a tutti i colleghi, anche a chi svolge mansioni diverse e in posizioni diverse.
La sicurezza del cittadino e dei diretti interessati dall'attività di impresa esige infatti un cambio di prospettiva: la *privacy* è sempre meno materia per avvocati e sempre più per *manager* esperti di sicurezza delle informazioni, di tecnologia, di organizzazione e processi aziendali.
Siamo di fronte a un profilo professionale che non può essere improvvisato e che richiede un notevole bagaglio di conoscenze e competenze che devono assicurare allo stesso tempo osservanza al Regolamento europeo, riservatezza e sicurezza.
La *data protection* è dunque una necessità da trasformare in opportunità di *business* e in un vantaggio competitivo.
Per questo, diciamo noi, il *data protection* officer deve essere innanzitutto un *manager*. Un *manager* che sappia prendere decisioni e fornire pareri, interfacciarsi con le esigenze aziendali, le norme del garante e, soprattutto, difendere il legame di fiducia che lega l'impresa al consumatore.

D.P.O

*Presidente Federmanager

COMMENTI & ANALISI

CONTRARIAN

COMPUTER VULNERABILI, INCIDENTE DI PERCORSO CHE FA PARTE DEL GIOCO

▶ La prima crisi della sicurezza informatica del 2018 è planata la settimana scorsa con un colpo a effetto. Alcuni ricercatori sulla sicurezza dei computer hanno scoperto significativi difetti nei microchip realizzati da vari produttori che alimentano ogni dispositivo moderno. Gli hacker potrebbero utilizzare queste vulnerabilità, definite con i soprannomi inquietanti Meltdown e Spectre, per succhiare le informazioni vitali da dispositivi che vanno dai giganteschi server aziendali al telefono tascabile. Panico. Alcuni allarmi catastrofici arrivano a dire che le correzioni di sicurezza necessarie rallenteranno le macchine a velocità non viste dai tempi del vecchio modem dial-up. Altri pensano che i difetti siano presenti così profondamente nei dispositivi che l'unica soluzione sia sostituirli, con un costo di centinaia di miliardi. Fermi tutti. Meglio fare un respiro profondo. Questi difetti sono tutt'altro che nuovi. Scoprire e affrontare tali problemi fa parte del ciclo di vita della tecnologia. La storia di Meltdown e Spectre è in realtà una buona notizia, in quanto riflette una crescente consapevolezza dell'importanza della cibersicurezza. L'industria ha creato processi sempre più robusti per ridurre al minimo il caos che gli hacker possono seminare utilizzando tali difetti e le notizie della scorsa settimana mostrano che questi processi funzionano. Per comprenderlo occorre rendersi conto che ogni tecnologia ha qualche difetto o vulnerabilità. Anche dopo aver speso molto tempo e denaro per togliere i bug dei dispositivi o del software prima del rilascio, gli esperti informatici calcolano che fino all'1% del codice sottostante comunque contiene errori. La consapevolezza dell'esistenza di questi difetti ha creato una gara tra ricercatori della sicurezza e hacker. Il problema è che, nonostante il tasso di vulnerabilità sia rimasto stabile o addirittura calato negli ultimi 20 anni, in termini assoluti queste vulnerabilità sono cresciute man mano che i dispositivi sono diventati inesorabilmente più complessi. Negli anni Settanta gli ingegneri scrissero circa 400 mila righe di codice per far volare lo Space Shuttle. Con un tasso di errore dell'1%, c'erano 4 mila possibili bug di sicurezza. Oggi uno smartphone tipico è alimentato da 10 milioni di linee di codice e un veicolo a motore medio ha dietro 100 milioni di linee di codice. Gli hacker lo sanno bene, ed è per questo che passano ore a pettinare i codici per trovare alcuni di questi 100 mila errori o più. Una volta trovato un difetto che possono usare per rubare informazioni o denaro, lanciano un virus informatico. Sapendo di che cosa sono capaci gli hacker, anche i ricercatori in tema di sicurezza sono costantemente alla ricerca dei difetti. Questo è uno degli aspetti positivi della storia di Meltdown e Spectre, purtroppo sottovalutato: i bravi ragazzi ci sono arrivati prima dei criminali. Gli esperti di sicurezza di tutto il mondo lavorano da almeno sei mesi per correggere questi difetti e proteggere i componenti vulnerabili. Molti sistemi critici hanno già regolato le loro difese per ridurre al minimo la possibilità di un attacco riuscito. Anche il Dipartimento americano della Homeland Security ha fatto la sua parte chiedendo rapidamente al settore privato di che cosa avesse bisogno e fornendo un archivio centrale di informazioni su come mitigare questa minaccia. Molto lavoro resta da fare, ma sembra che si sia alcuni passi avanti rispetto agli hacker. La cosa più importante è mantenere il costante stato di allerta e reattività che hanno portato Meltdown e Spectre all'attenzione mondiale. Se non riusciamo a mantenere ben alta la nostra guardia virtuale, la prossima grande vulnerabilità cibernetica potremmo apprenderla dai cattivi.

THE WALL STREET JOURNAL.

La nuova rivoluzione industriale non risparmierà il mercato immobiliare. Anzi

DI HUGO MACHIN*

Il mondo sta cambiando a un ritmo che non si vedeva dalla prima Rivoluzione Industriale. Ciò ha profonde conseguenze sui luoghi in cui viviamo e sul nostro modo di utilizzare gli immobili. Con il processo di industrializzazione mondiale, a metà del XIX secolo le nuove fabbriche hanno avuto bisogno di investimenti per crescere. Un aspetto cruciale è che banchieri, avvocati e contabili che li hanno resi possibili non dovevano essere sul posto. Le competenze specialistiche hanno iniziato a comparire nei grandi centri urbani: le città. Con l'avvento delle nuove tecnologie (basse tariffe postali, telefono e illuminazione elettrica), gli edifici in città hanno potuto continuare a servire l'industria pesante situata in luoghi più lontani. Il progresso tecnico come catalizzatore della nascita dei centri urbani è stato un punto di svolta per la storia delle nostre città. Ora si è a un secondo punto di svolta. Le analogie che individuiamo oggi riguardano le dimensioni delle società che dominano l'economia e la vita quotidiana. Naturalmente, parliamo di società tecnologiche. A differenza di quanto avveniva nel XIX secolo, quando i maggior datori di lavoro erano ubicati fuori dai centri urbani, oggi le grandi società hi-tech devono trovarsi in città. Ciò accresce o riduce la domanda di certi spazi. È quello che chiamiamo ricentralizzazione.
I colossi tecnologici sono importanti datori di lavoro e necessitano di forze lavoro numerose e istruite. A differenza dei grandi gruppi della rivoluzione industriale, le società digitali devono trovarsi in città per attrarre collaboratori dotati delle qualifiche richieste e sfruttare i trasporti di massa per portare i dipendenti sui posti di lavoro. La tecnologia induce la ricentralizzazione.
Tale richiesta determina il successo di determinate città. Si assiste a una biforcazione del vigore economico delle Global City, con un numero crescente di centri regionali che viene emarginato. Solo poche città saranno in grado di ospitare i grandi datori di lavoro, e ciò determinerà uno scenario in cui chi vince prende tutto.
Oltre a essere importanti fonti di occupazione che incidono sulla solidità economica dei centri urbani, con i loro prodotti le imprese tecnologiche influiscono sull'evoluzione della domanda di immobili nelle città che le ospitano. La tecnologia sta cambiando il modo in cui questi sono utilizzati. Prendiamo l'e-commerce. Oggi negli Stati Uniti il 16% di tutte le vendite al dettaglio avviene online.
Questo fenomeno sta trasformando le vendite al dettaglio tradizionali. Se l'84% della spesa non avviene sul web, allora la strada è ancora molto lunga prima che i più giovani fruitori dell'e-commerce sostituiscano gli acquirenti più tradizionali; a oggi, stiamo già assistendo al fallimento di numerosi grandi magazzini e molte altre aziende soccombono al potere di Amazon: tuttavia, i dati lasciano presagire che questo sia solo l'inizio.
Ancora una volta, le analogie con la Rivoluzione Industriale sono evidenti. Nell'epoca vittoriana, il progresso nel settore manifatturiero ha fatto emergere nuove aree di domanda, causando profondi cambiamenti sociali. Tornando ai giorni nostri, la tecnologia influisce su quasi tutti gli aspetti della nostra vita e traccia nuovi confini. Il modo in cui facciamo acquisti, viaggiamo, comunichiamo e reperiamo le informazioni coinvolge in misura crescente i dispositivi portatili.
Le conseguenze di questa trasformazione determinano i rendimenti degli investimenti.
L'uso e l'adozione delle nuove tecnologie sta trasformando il mercato immobiliare e questa domanda si manifesta nei centri dei consumi di massa: le città. Facciamo alcuni esempi. La domanda di spazi logistici è aumentata perché necessari a gestire le spedizioni ordinate online; i data center sono sempre più richiesti in quanto vi è trasferita e conservata una mole maggiore di dati; la domanda di provider di uffici flessibili ha guadagnato terreno per soddisfare modelli di lavoro diversi. D'altro canto è diminuita la domanda di punti vendita al dettaglio fisici e di uffici decentralizzati.
Ciò conferma che, se non teniamo in portafoglio il giusto tipo di immobili, esiste il rischio molto concreto che la tecnologia faccia ai nostri investimenti ciò che Amazon ha già fatto al commercio di libri e che Uber sta facendo ai servizi di taxi. I confini vengono ridefiniti, gli innovatori irrompono sul mercato e il mercato immobiliare non è immune a questa dinamica. Non crediamo che questo cambiamento sia alle battute finali, anzi: osserviamo tutta una serie di grandi cambiamenti che iniziano appena a manifestarsi.

*co-Head of Global Real Estate Securities, Schroders

Perché un cyberattacco sarà ben più costoso

DI VINCENT VANDENDAEL*

Il nuovo Regolamento europeo sulla privacy entrerà in vigore tra sei mesi. L'obiettivo è creare una struttura coordinata sulla protezione dei dati per tutta l'Ue. La sua attuazione darà ai cittadini molti più poteri rispetto al modo con cui i loro dati sono raccolti e gestiti, incluso il tanto discusso diritto all'oblio. Il nuovo Regolamento darà vantaggi notevoli ai consumatori ma allo stesso tempo darà rilevanti problemi alle aziende, in particolare per le conseguenze finanziarie degli attacchi informatici. Violazioni dei dati causano sempre perdite finanziarie, e per vari motivi: perdita di clientela, blocco dell'attività, danni alla reputazione. Il nuovo Regolamento europeo (Gdpr) renderà le conseguenze ancora più significative. Le aziende che non rispetteranno i termini del nuovo regolamento o subiranno una violazione informatica, potrebbero dover far fronte a multe fino a 20 milioni di euro o al 4% del fatturato annuale. In Italia l'ammontare dei pagamenti effettuati nel 2016 da parte dei soggetti verso i quali sono stati avviati procedimenti sanzionatori è risultato pari a 3.3 milioni di euro e nel 2017 il Garante italiano ha emesso la più alta sanzione, pari a 11 milioni di euro, nell'ambito dell'Unione Europea per la violazione della normativa privacy. L'entrata in vigore del nuovo regolamento Ue è destinata ad aumentare le sanzioni, basti pensare che gli esperti di cybersicurezza del Gruppo Ncc hanno stimato che le multe comminate dall'Information Commissioner's Office (Ico) alle compagnie britanniche lo scorso anno avrebbero toccato i 69 milioni di sterline, anziché 880.500 se il Gdpr fosse già stato in vigore. Non è una differenza insignificante: le multe multimilionarie possono far uscire le aziende dal mercato. I rischi di un attacco sono sempre presenti e l'impatto potenziale sarà molto più serio tra sei mesi. Un'ovvia risposta a questa minaccia è aumentare la spesa per la sicurezza informatica e creare barriere protettive più forti. Di sicuro un passo nella giusta direzione e le aziende che potranno dimostrare di aver adottato tali misure saranno valutate in modo più favorevole dalle Autorità.
Le aziende europee lavoreranno intensamente nei prossimi mesi per garantire la loro conformità e preparazione al Gdpr. I nuovi regolamenti rappresentano anche un'opportunità per tutte le organizzazioni per accertarsi di avere a portata di mano le competenze necessarie a difendersi da un attacco informatico, salvaguardando l'attività aziendale.
Ma ci sono limiti oggettivi a quanto le organizzazioni possono fare. Secondo una recente indagine dei Lloyd's, *Facing the Cyber Risk Challenge*, il 92% degli intervistati europei conferma che la loro azienda ha subito violazioni dei dati negli ultimi 5 anni. Un hacker può arrivare a penetrare firewall e altre protezioni, come dimostrato da violazioni di alto profilo ai danni di enti come il Pentagono. In realtà è più un problema di quando, piuttosto che di se, un'azienda sarà vittima di un cyberattacco.
Se non è possibile garantire la sicurezza alzando il livello di protezione, cosa si può fare per ridurre l'impatto di una violazione dei dati?
Per la maggior parte delle aziende la portata e la gravità delle multe imponibili, in linea con il Gdpr, in caso di violazione dei dati sono semplicemente troppo pesanti per essere sostenute. Le aziende che vogliono essere preparate al meglio dovranno dunque cercare di mitigare i rischi legati a un cyberattacco e ridurre il costo dei premi, affidandosi ad un assicuratore specializzato. Assicurarsi dovrebbe essere il primo importante passo. Lavorando con esperti di sicurezza informatica e assicuratori, le aziende potranno valutare meglio i rischi e ridurli, proteggendo non solo il conto economico ma anche la reputazione.

*chief commercial officer, Lloyds

Il Sole 24 Ore
Giovedì 22 Febbraio 2018 - N. 52

Dati. A tre mesi dall'entrata in vigore del regolamento

Privacy, in ritardo una impresa su due

Enrico Netti
MILANO

Italia maglia nera nel percorso di avvicinamento al Gdpr. A tre mesi dall'entrata in vigore del regolamento europeo per la protezione dei dati una impresa italiana su due non dispone ancora di un piano per adeguarsi agli obblighi in materia di privacy. Tra le principali economie dell'area Ue solo la Francia è al nostro stesso livello, la media europea è del 60% ma in Germania si arriva all'80%, nel Regno Unito al 68% e in Irlanda sono *compliant* tre aziende su quattro. È quanto emerge dal sondaggio «Global forensic data analytics 2018» realizzato da Ey. «In questo quadro la posizione dell'Italia non rassicura anche alla luce delle pesanti sanzioni previste – osserva Fabrizio Santaloia, partner Ey e responsabile dei "Fraud investigation & dispute services" –. Un aiuto può arrivare dagli strumenti di Forensic data analytics (Fda *ndr*) che consentono di identificare minacce e rischi e di essere conformi alle norme».

Nel nostro paese il 67% del campione ritiene che gli strumenti Fda abbiano un ruolo chiave per affrontare le cyber minacce e la parte restante pensa siano comunque efficaci. A livello globale in quest'area si concentrano gli investimenti che segnano un +51% della media annua rispetto al 2016 mentre in Italia il trend è inferiore. In altre parole nelle aziende più strutturate si stanno implementando soluzioni a base di intelligenza artificiale, con software "robot" che automatizzano in modo radicale l'attività di monitoraggio del perimetro aziendale e provvedono all'analisi evoluta dei dati raccolti. Con questi strumenti, insegna l'esperienza maturata all'estero, si riescono a gestire gli obblighi del Gdpr, i rischi legali e le frodi. L'adozione di queste piattaforme robot, secondo il sondaggio, è già una realtà in poco più di un terzo delle grandi aziende italiane mentre l'intelligenza artificiale è già stata scelta dal 18% del campione. Nell'arco dei prossimi dodici mesi questi strumenti diventeranno sempre più diffusi.

60%

Media europea
Quota di imprese Ue che si sono adeguate agli obblighi del Gdpr

Una evoluzione che porta a un gap tra le risorse specializzate già presenti in azienda e le competenze che devono operare con le nuove piattaforme. «Il 60% delle società italiane dichiara di non disporre di personale dedicato contro il 39% a livello globale» conclude Santaloia.

enrico.netti@ilsole24ore.com

COMMENTI & ANALISI

CONTRARIAN

La Serie A considera che i diritti tv della Premier costano meno

▶ Un monito. Un campanello d'allarme da non trascurare. Perché se la Premier League è il non plus ultra per quel che riguarda la vendita ,a valori stellari, delle immagini del calcio giocato in Europa, allora bisogna prestare molta attenzione a quello che è successo in questi giorni. Per due (buone) ragioni. Innanzitutto, il fatto che al bando si sono presentati solo due competitor: Sky e British Telecom. E in seconda istanza, il fatto che questi due operatori hanno messo complessivamente sul piatto una cifra inferiore rispetto alle attese e soprattutto all'incasso del bando precedente. Ne devono prendere atto sia i 20 club della Serie A, sia il commissario della stessa Confindustria del pallone, ovvero Giovanni Malagò, numero 1 del Coni, sia l'advisor Infront, sia, infine, l'intermediario unico che mettendo sul piatto 1.000 euro in più del minimo richiesto, ovvero 1,05 miliardi su base annua, che invece contano di fare il tutto esaurito e trovare molti più operatori tv, tlc e Ott a cui rivendere i diritti tv 2018-2021 rispetto alle sole e solite Sky e Mediaset Premium. Nello specifico, la Premier League ha ceduto cinque dei sette pacchetti di partite per il triennio 2019-2022 per un importo totale di 4,46 miliardi di sterline, una soglia inferiore rispetto ai 5,12 miliardi incassati con la precedente asta. Un traguardo difficile da raggiungere anche se devono ancora essere assegnati due pacchetti (in passato venduti a 250 milioni di sterline ciascuno) a 5,62 miliardi di euro. In particolare Sky, che tra Inghilterra e Irlanda ha 12,9 milioni di abbonati (il 57,3% dell'intero parco-clienti europeo), ha speso 3,58 miliardi di sterline per aggiudicarsi comunque 128 match, due in più del precedente bando, risparmiando in totale ben 521 milioni (il 12,7%) rispetto a quanto speso la volta precedente. Come si spiega questo passo indietro del campionato più ricco d'Europa? Una prima risposta va trovata nei player presentatisi ai nastri di partenza. Sempre e solo due, ovvero l'unica pay tv satellitare del mercato e il big della telefonia locale. Di altri operatori televisivi o telefonici non se ne sono visti. Così come non si sono palesati, nonostante l'importanza del business e la lingua inglese, gli over-the-top tanto attesi, a partire da Netflix (che ruba manager a major cinematografiche e broadcaster ma non si mette a produrre e distribuire calcio) e Amazon. Un elemento da tenere in considerazione è che si dovranno cercare compratori delle immagini della Serie A, campionato che continua a perdere spettatori, che non trova né un presidente né un amministratore delegato e che a livello europeo non vince una competizione dal 2010 (Inter). Per non parlare della disfatta della Nazionale italiana, fuori dai Mondiali di Russia. Non va trascurato poi il fatto che pure sul mercato locale soggetti veramente interessati sono da sempre solo due: Sky e Mediaset Premium. Mentre né Tim né Vodafone hanno mai trasmesso partite. Per non parlare degli Ott che finora non si sono mai palesati e probabilmente mai lo faranno. Elementi da non sottovalutare per una Mediapro che ora diventa cinese (come i proprietari di Milan e Inter) ma che ieri è stata pizzicata dall'Antitrust spagnolo, che ha imposto all'intermediario, che sul mercato iberico ha anche canali tematici (Gol e BeIn Sports), di aprirli alle piattaforme online, senza discriminarle per quel che riguarda i diritti della Lega e della Champions League.

Giovanni Malagò

Oggi a Baku si ridefinisce l'assetto del mercato del gas nell'Europa Meridionale

DI DANIELE LAZZERI*

L'energia, oltre a essere fondamentale per la sicurezza e lo sviluppo di un Paese, è anche un settore in continua evoluzione grazie all'applicazione di sempre più avanzate tecnologie, che nel tempo hanno rivoluzionato le tecniche di estrazione dei combustibili e ne hanno ampliato la distribuzione in vaste aree del pianeta.
Un importante round della grande partita energetica globale avrà luogo a Baku. La capitale dell'Azerbaigian, ospiterà infatti oggi la quarta riunione ministeriale del Consiglio Consultivo del Corridoio Meridionale del Gas. L'Azerbaigian già da anni è importante per la sicurezza energetica dell'Europa come fornitore di greggio, soprattutto per l'Italia di cui nel 2017 è stato il principale fornitore. Baku vede costantemente accrescere il suo ruolo internazionale e oggi è anche un'illustre candidata a ospitare l'Expo 2025, forte dello slogan «Sviluppare il capitale umano, costruire un futuro migliore». Questo dopo che a Milano 2015 il padiglione dell'Azerbaigian è stato tra i più apprezzati. Presso l'Heydar Aliyev Centre, frutto della matita di Zaha Hadid, avrà luogo la riunione di oggi, dedicata all'attuazione del Corridoio Meridionale del Gas. L'incontro giunge in un momento di particolare rilevanza, visto che il corridoio diventerà operativo nel 2018, con il flusso del primo gas previsto già quest'anno. Alla convention parteciperanno i ministri dell'Energia dei Paesi attraversati dal corridoio insieme ai rappresentanti della Commissione Ue e del governo Usa. Sia Washington che Bruxelles, infatti, si sono spesi per migliorare la sicurezza energetica europea. Il Southern Gas Corridor è un progetto geopolitico del valore di 40 miliardi di dollari, cui partecipano sette Paesi. Sono 11 gli investitori, inclusa l'italiana Snam, e 12 i buyer coinvolti nel progetto. Le importazioni e la domanda di gas in Europa sono in costante aumento, e il Southern Gas Corridor dovrà soddisfare parte di questa nuova domanda, consentendo alle centrali elettriche di abbandonare l'utilizzo del carbone. Con l'avvio dei flussi di gas quest'anno, la Socar (società statale dell'Azerbaigian) e i suoi partner nel Corridoio stanno ora valutando una fase 2, in cui saranno raggiunti ulteriori mercati, con un occhio di riguardo alla penisola balcanica. Ma il Consiglio consultivo vede per la prima volta anche la presenza di esponenti della Romania, con l'obiettivo di raggiungere molte delle isole energetiche europee. Sullo sfondo la necessità di diversificare le fonti di approvvigionamento energetico come previsto dalla Strategia Energetica Nazionale (Sen). Ne abbiamo avuto immediata percezione con il guasto al gasdotto Tag (Trans Austria Gasleitung) a inizio dicembre. La temporanea sospensione nell'erogazione di gas che – attraverso Tarvisio – giunge in Italia è stato un significativo campanello d'allarme sulla stabilità delle forniture. Condivisibili le preoccupazioni del ministro dello Sviluppo Economico, Carlo Calenda, che ha sottolineato come l'Italia – in assenza di altre fonti di approvvigionamento – avrebbe solo pochi giorni di autonomia, scaduti i quali la prospettiva per la nazione sarebbe restare al freddo e al buio. Una situazione risolvibile solo con un'attenta politica di riduzione della dipendenza energetica tramite la moltiplicazione delle fonti di fornitura. Il positivo impatto sulla loro stabilità, peraltro, consentirebbe anche una contestuale diminuzione dei prezzi della materia prima grazie alla concorrenza, con il conseguente aumento della competitività delle imprese italiane e un sollievo per le famiglie, che vedrebbero ridursi la bolletta energetica.
Ma la sicurezza è un tema dalla doppia accezione: stabilità degli approvvigionamenti da un lato, ma anche sicurezza dell'infrastruttura. Per esempio, l'ultimo tratto del Corridoio, il gasdotto Tap (Trans Adriatic Pipeline) che raggiungerà le coste italiane, è stato progettato in base ai migliori standard internazionali e realizzato con tecnologie all'avanguardia. Ciononostante, si riscontrano ancora oggi resistenze alla realizzazione di un'opera che, per dimensioni economiche e valenza geopolitica consentirebbe all'Italia di diventare un hub del gas per l'Europa. Non è un caso che il progetto sia stato riconosciuto dall'UE come un Progetto di interesse comunitario. (riproduzione riservata)

**presidente del think tank Il Nodo di Gordio*

Quanta confusione regna sulla privacy

DI MARINO LONGONI

Solo un terzo delle aziende è in regola con le norme del nuovo regolamento europeo sulla privacy, che diventeranno pienamente operative a partire dal 25 maggio 2018: si tratta in gran parte di banche e società di informatica o telecomunicazioni. Il bicchiere mezzo vuoto emerge da una recente ricerca di Dla Piper. Ma c'è anche quello mezzo pieno, come riporta un'indagine dell'Osservatorio del Politecnico di Milano: in più della metà delle imprese è in corso un processo di adeguamento alle nuove regole e un altro terzo sta studiando il da farsi. Si può dire quindi che il mondo del business, pur in ritardo, si sta muovendo (e questo sembra essere un dato comune in tutta Europa), ma non sarà certamente possibile colmare questo gap nei prossimi tre mesi. Con la conseguenza che dal 25 maggio in molti si troveranno esposti al rischio di sanzioni draconiane: fino a 20 milioni o il 4% del fatturato globale.
In realtà, in grave ritardo è anche la Pubblica amministrazione, non solo perché gli enti pubblici sono tra i più lenti a implementare le regole per la sicurezza informatica e la protezione dei dati degli utenti, ma soprattutto perché la Pa ha accumulato gravi ritardi nella definizione delle norme che devono essere osservate dai cittadini e dalle imprese, tanto che il Gdpr (General data protection regulation) è sotto molti aspetti un cantiere ancora aperto. Per esempio, la legge 163 del 2017, all'articolo 13 delega il governo alla scrittura delle regole di raccordo interno tra regolamento europeo e norme italiane: questioni delicate in materia sanitaria, e anche per molte pubbliche amministrazioni, o in materia di applicazioni di sanzioni. È vero che ci sarebbe tempo fino a maggio ma in questo momento non c'è ancora niente, nemmeno le bozze dei decreti legislativi, tranne quello sulla giustizia. Ci sono anche molti adempimenti delle imprese in attesa di provvedimenti attuativi da parte delle autorità europee. Per esempio, quelle che trattano dati con rischi elevati per le persone dovrebbero compilare un documento che si chiama valutazione di impatto privacy, ma è tutto ancora fermo in attesa che il Garante italiano, sulla base delle indicazioni che dovrebbero arrivare da quelli europei, spieghi chi è tenuto e chi no. Oppure, non è ancora chiaro, in molti casi, come si deve chiedere il consenso. Manca ancora un format per il contratto tipo per la nomina del responsabile esterno del trattamento (quando si affidano attività in outsourcing) e non sono state definite le icone che possono essere utilizzate per l'informativa sulla privacy.
E non basta. Ci sono provvedimenti italiani successivi al regolamento europeo che sono a rischio di incompatibilità: per esempio la legge Bilancio 2018 (n. 205/2017), ai commi 1022 e 1023 ha precisato quando le imprese possono effettuare trattamento di dati senza chiedere il consenso, ma mentre per il regolamento europeo basta che l'azienda autocertifichi di avere un legittimo interesse in questo senso, secondo la norma italiana, successiva al regolamento, è necessario fare una specifica richiesta al Garante per ottenere l'esonero. È difficile adeguarsi a norme mancanti o non chiare. Tuttavia sembra che la maggior parte delle imprese si stia almeno rendendo conto che il problema esiste. E non solo quello della privacy, ma più in generale quello della protezione dei dati personali che, ormai, sono diventati più preziosi dell'oro, ma che proprio per questo hanno bisogno di tutela adeguata. E spesso non basta nemmeno essere in regola con le norme vigenti, perché l'evoluzione tecnologica è molto più veloce di quella normativa e apre sempre nuove opportunità ai malintenzionati di tutti i tipi. È una battaglia tra guardie e ladri combattuta apparentemente senza spargimento di sangue. Ma i danni che si possono provocare con la pirateria industriale o con il furto di informazioni, sono enormi. Potrebbe, forse, essere il caso di introdurre, per chi tratta dati riservati, un obbligo di assicurazione obbligatoria (simile a quella sulla Rc auto), anche per aumentare la consapevolezza sul valore dei dati stessi e sulla necessità di trattarli in modo adeguato. (riproduzione riservata)

GDPR/1. Dal 25 maggio in vigore il regolamento europeo sull'utilizzo dei dati in Internet

Una rivoluzione annunciata

Per le aziende non si tratta solo di adempimenti, ma soprattutto di una nuova filosofia che costringe a ragionare su come si usa la tecnologia e a mettere ordine nel data base... poche però l'hanno compreso

di **Giovanni Medioli**

È il caso di dirlo: il silenzio sulla prossima entrata in vigore (dal 25 maggio) del Gdpr (Regolamento Ue 2016/679) sull'accesso alla rete e la protezione dei dati personali è assordante. Probabilmente distratti da una campagna elettorale brutta, sporca e cattiva i giornali italiani sembrano non essersi nemmeno accorti che sta per diventare legge anche in Italia una delle norme più importanti e invasive per la vita di tutti che si ricordino nell'ultimo decennio. Si tratta del nuovo regolamento europeo per l'utilizzo dei dati personali di persone e aziende che qualsiasi organizzazione "detiene" sui suoi database. In pratica, regola l'utilizzo della rete a fini commerciali (e non solo). Ovvero un intero nuovo schema legislativo che regolerà la vita di tutti (ma in particolare delle imprese) rispetto a Internet. Da notare: non si tratta di una direttiva, con tempi lunghi (e incerti) di recepimento da parte delle nazioni che fanno parte dell'Unione e montagne di regolamenti attuativi da definire, prima che si possano vedere i suoi effetti.

Regole e sanzioni per tutti, senza distinzioni

È un regolamento dell'Unione, approvato nel maggio 2016 con due anni di periodo transitorio, vincolante per tutti. Dal 25 maggio sarà immediatamente legge vigente in tutti i 26 stati membri (e, come vedremo, con effetto anche sul Regno Unito, malgrado la Brexit), che devono istituire un'apposita Authority di vigilanza (nei fatti sono le Authority sulla privacy che assumeranno questo ruolo, inglobando anche funzioni di controllo sulla sicurezza dei dati – *cibersecurity* – per cui hanno già ricevuto un finanziamento dalla Commissione) e riguarda tutte le organizzazioni (enti, aziende, professionisti), non solo con sede nell'Unione ma anche con sede fuori dall'Europa che operano nell'Unione offrendo beni o servizi, come viene spiegato in maniera molto chiara nella relativa pagina web (https://www.eugdpr.org/). Già definite anche le sanzioni per le violazioni della nuova norma, che consistono in multe fino al 4% del fatturato delle aziende "beccate" a violare le nuove norme, sino a un massimo di 20 milioni di euro (per i semplici dati non in ordine le multe saranno pari al 2% del fatturato). Sanzioni che, bisogna ricordarlo, non distinguono fra Pmi (per le quali potrebbero essere letali) e giganti come gli Ott (i soliti Apple, Google, Microsoft, Facebook, Amazon...), per i quali anche la sanzione massima potrebbe essere solo un "incidente di percorso".

Cosa cambia per le imprese

La gestione e i diritti relativi ai dati personali, dove per "dati personali" si intende qualsiasi informazione sensibile che consenta l'identificazione e/o la profilazione del cittadino, a cominciare da nome, indirizzo fisico o e-mail, foto, dettagli sulla posizione bancaria, post sui social, informazioni mediche, l'IP di un computer. Questa denominazione, di fatto, sostituisce quella più circoscritta di "dato sensibile" in vigore in Italia fino a oggi.

Le aziende che gestiscono i dati personali, in base alla nuova legge, dovranno:

- **comunicare le violazioni dei dati personali** (*Data Breaches*), cioè gli accessi non giustificati ai dati custoditi, le fughe di notizie, all'autorità nazionale preposta e agli interessati, ogni volta che "ne risulti un rischio per i diritti e la libertà degli individui" entro 72 ore dall'avvenuta violazione;
- **garantire il diritto all'accesso** all'interessato dei propri dati personali;

- **garantire il diritto all'oblio.** Basta con le sentenze inappellabili che rimangono per sempre accessibili in rete: era legge anche prima, ma adesso diventa un diritto molto più concreto;
- **garantire la portabilità dei dati** ovvero che i dati personali siano non solo accessibili e utilizzabili dal titolare, ma anche "spendibili" in altri contesti semplicemente su richiesta;
- **garantire in maniera strutturale la privacy** dei dati trattati. La privacy non è un "pezzo" che viene aggiunto ai nostri dati personali, ma deve essere la maniera in cui questi dati nascono e vengono trattati fin dal principio. I princìpi di *Privacy by Design and by Default* (Articolo 25) richiedono infatti che la protezione dei dati faccia parte del progetto di sviluppo dei processi aziendali per tutti i prodotti e servizi, e le impostazioni di privacy sono configurate su un livello alto in modo predefinito. Inoltre è l'azienda che deve essere in grado di spiegare perché deteneva quei dati. Se i dati, ancorché obsoleti, sono in un database che viene violato, in altre parole l'azienda o l'ente che possiede il database deve poter dimostrare che quei dati erano lì per una ragione specifica e legittima, altrimenti scatta la sanzione;
- **dotarsi di un responsabile della protezione dei dati** (Dpo, Data protection officer), che è una nuova figura specifica e ben distinta da chi si limita a gestire i dati, se l'azienda rientra nelle categorie a cui viene fatto obbligo di avere una simile figura. Le aziende su cui grava quest'obbligo sono: tutte le Pubblice Amministrazioni a qualsiasi livello (dunque dai ministeri fino al più piccolo dei comuni), le aziende che raccolgono dati dal pubblico su vasta scala (in sostanza chiunque venda beni o servizi al pubblico e abbia un elenco di clienti), le aziende che trattano strutturalmente i dati personali dei loro clienti/utenti/interlocutori (fra le altre certamente call center, banche, Sgr, assicurazioni, ospedali, studi di analisi mediche, ma anche società di selezione e gestione del personale, corrieri e operatori logistici ecc.). Il Dpo è direttamente responsabile, fra l'altro, della comunicazione al garante e agli interessati (cioè i titolari dei dati che sono stati rubati) delle eventuali violazioni, entro 72 ore dalla scoperta della violazione stessa. Gli interessati, peraltro, devono avere la possibilità di interagire con questa figura per tutti i problemi che riguardano la gestione dei loro dati personali.

La richiesta di consenso

Dal momento dell'entrata in vigore della legge l'azienda che tratta i dati personali dei clienti/interlocutori dovrà ottenere dall'interessato un consenso "esplicito" e "non ambiguo" al trattamento dei dati stessi. In altre parole le aziende non potranno più (come è specificato nella legge) sottoporre al cliente lunghi e illeggibili "termini e condizioni" scritti in pagine e pagine di legalese. La richiesta di consenso dovrà essere "intellegibile e facilmente accessibile" e contenere in maniera inequivocabile "lo scopo per cui si chiede di poter utilizzare i dati personali" espresso in maniera "non ambigua". "La richiesta di consenso deve essere chiaramente distinguibile da altre materie e posta in una forma chiara e facile da comprendere, utilizzando un linguaggio chiaro e semplice". Non saranno ammesse peraltro formule non specifiche o semplificazioni eccessive come "clicca qui". Per la vendita o fornitura di servizi o beni online a minori di 16 anni diventa obbligatorio il consenso esplicito dei genitori o di chi ne fa le veci. Gli Stati membri possono decidere di abbassare l'età del consenso, comunque non al di sotto dei 13 anni. Il consenso non sarà più "per sempre", ma avrà una "data di scadenza" specifica a seconda dell'uso previsto per i dati. Dopo quella data dovrà essere rinnovato.