Aspetti legali della sicurezza informatica

Aspetti legali della sicurezza informatica

Gli ultimi anni sono stati estremamente rilevanti sotto il profilo dell'evoluzione normativa in materia di sicurezza informatica in quanto diverse sono state le novità che si sono succedute nel tempo e non tutte andate nella medesima direzione. Il futuro potrebbe inoltre apportare ulteriori cambiamenti in questo ambito nel caso si giungesse, nel corso dell'anno 2016, all'approvazione del Regolamento Europeo in materia di privacy il cui iter è iniziato nel gennaio del 2012. Tale Regolamento andrebbe a sostituire la Direttiva n°45/96 da cui promana anche la legislazione italiana in materia di privacy. Se così sarà, il tema della sicurezza dei dati personali aumenterà di rilevanza in maniera esponenziale, in quanto le previsioni ivi contenute sono particolarmente stringenti e prevedono, tra l'altro, l'adozione di una politica della sicurezza con obbligo quindi per aziende e pubbliche amministrazioni di prestare altissima attenzione al problema. Lo schema di Regolamento attualmente disponibile sta già condizionando gli operatori economici, interessati a non farsi trovare impreparati rispetto ad adempimenti sicuramente più gravosi di quelli attuali.

Avendo il presente contributo lo scopo di delineare a livello generale la tematica della sicurezza informatica e le ultime tendenze della regolamentazione in materia, si ritiene opportuno partire dai principi fondamentali in questo ambito. Indubbiamente la normativa che ha l'impatto maggiormente rilevante sul tema che stiamo trattando è quella relativa al trattamento dei dati personali, contenuta nel d.lgs. 196/2003, che ha introdotto specifici obblighi di sicurezza. In particolare, si sottolinea come questa norma abbia introdotto il principio generale di idoneità delle misure di sicurezza. I dati personali, infatti, devono essere custoditi e controllati (anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento) in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31 d.lgs. 196/2003). In altri termini, le misure di sicurezza andrebbero valutate sulla base dell'analisi dei dati personali che vengono trattati e dei rischi specifici che incombono sugli stessi, nella consapevolezza che la normativa, nel caso il trattamento dei dati generi un danno a terzi, obbliga il titolare al risarcimento del danno, ove non riesca a dimostrare di aver adottato tutte le misure idonee ad evitarlo. Questo principio è confermato dallo schema di Regolamento europeo in materia di privacy in base al quale "*Chiunque subisca un danno, incluso un danno non pecuniario, cagionato da un trattamento illecito o da altro atto incompatibile con il regolamento ha il diritto di chiedere il risarcimento del danno dal responsabile del trattamento o dall'incaricato del trattamento*"; il Data Controller (corrispondente al Titolare del Trattamento, in base alle definizioni della normativa vigente) o il Data Processor (Responsabile del trattamento) possono essere esonerati in tutto o in parte da tale responsabilità se provano che l'evento dannoso non è loro imputabile. Ed un atto incompatibile con il Regolamento potrebbe proprio essere la mancata adozione di un livello idoneo di sicurezza, posto che la normativa europea rafforza ulteriormente l'approccio basato sul rischio disponendo che il Data Controller ed il Data Processor devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta, tenuto conto dei risultati della valutazione di impatto in materia di protezione dei dati e dell'evoluzione tecnica e dei costi di attuazione.

Purtroppo, nel corso del tempo, si è assistito ad un'eccessiva sottovalutazione del principio generale di adozione delle misure idonee di sicurezza rispetto ad una più attenta supervisione degli obblighi di adozione delle misure minime di sicurezza, espressamente elencate dal Codice Privacy (artt. 33 e ss. ed

Allegato B), forse in considerazione della deterrenza derivante dall''impatto sanzionatorio applicabile (sanzioni di carattere penale ed amministrativo) che prescinde dalla verificazione di un danno. Occorre comunque considerare che lo schema di Regolamento europeo in materia di privacy, a differenza della disciplina italiana vigente, non prevede misure minime di sicurezza a protezione dei dati personali. Se confermato, quindi, il Regolamento comporterà inevitabilmente un cambiamento di prospettiva per i destinatari.

Fatto cenno ai principi generali della normazione in materia di sicurezza informatica, si rileva che negli ultimi anni, a fronte di alcuni interventi normativi mirati ad aumentare gli obblighi di sicurezza all'interno delle imprese e della pubblica amministrazione italiana, alcune scelte hanno portato invece a una diminuzione degli obblighi e quindi, potenzialmente, a una riduzione dell'attenzione sul problema degli attacchi informatici interni e esterni. Nel Rapporto Clusit 2015 si legge "*In uno studio condotto nel corso del 2014 sono state monitorate su scala globale 1.600 aziende appartenenti a 20 diversi settori merceologici, osservando che nel periodo considerato, in media, la percentuale di organizzazioni compromesse è stata superiore al 90%, con alcuni particolari settori (Legal, Healthcare e Pharma, Retail) che hanno avuto un tasso di compromissione del 100%*", a testimonianza del fatto che l'attenzione sui rischi informatici, indipendentemente dagli obblighi normativi, deve sempre essere altissima.

Fatte queste premesse vediamo allora quali sono le linee di tendenza del legislatore e dell'Autorità Garante per la protezione dei dati personali che è possibile cercare di individuare nell'evoluzione normativa.
In prima battuta sembra possibile intravedere la scelta di passare da una normativa tendenzialmente identica per tutti i settori di mercato all'introduzione di provvedimenti settoriali mirati a imporre maggiori oneri e adempimenti in tema di sicurezza informatica per quelle categorie di operatori economici che sono più esposti a rischi e rispetto ai quali una violazione della sicurezza potrebbe maggiormente impattare sul cittadino.

Nella direzione della semplificazione sono andati, per esempio, i provvedimenti che hanno portato all'abrogazione del cosiddetto Decreto Pisanu, all'eliminazione dal perimetro di tutela della normativa in materia di trattamento dei dati personali inerenti le persone giuridiche, enti, associazioni, alla scelta di eliminare del tutto e per tutti l'obbligo di stendere annualmente il documento programmatico sulla sicurezza, e l'individuazione per legge dei trattamenti con finalità amministrativa-contabile che ha di fatto portato alla limitazione del perimetro di applicazione del Provvedimento del Garante per la protezione dei dati personali in materia di amministratori di sistema del 27 novembre 2008, confinandolo, nel suo ambito di obbligatorietà, ad un perimetro estremamente ridotto.

Di contro, i provvedimenti emanati ad hoc per specifici settori di mercato sono stati estremamente rilevanti e se ne citano qui solo due di maggior rilievo:

- Provvedimento del Garante per la protezione dei dati personali in materia di tracciamento degli accessi ai dati bancari (Provvedimento n° 192/2011)
- Decreto legislativo n° 69/2012 che ha introdotto per le società di telecomunicazione l'obbligo della segnalazione dei data breach.

In particolare, il Provvedimento del Garante 2011 ha imposto che le Banche, oltre alle misure minime di sicurezza già prescritte dal Codice nel caso di trattamento di dati personali effettuato con strumenti

elettronici, debbano implementare misure idonee che permettano un efficace e dettagliato controllo anche in ordine ai trattamenti condotti sui singoli elementi di informazione presenti nei diversi database utilizzati.

Tali soluzioni devono comprendere la registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari, quando consistono o derivano dall'uso interattivo dei sistemi operato dagli incaricati, sempre che non si tratti di consultazioni di dati in forma aggregata non riconducibili al singolo cliente. I file di log devono tracciare, per ogni operazione di accesso ai dati bancari effettuata da un incaricato, almeno le seguenti informazioni: il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso, la data e l'ora di esecuzione, il codice della postazione di lavoro utilizzata, il codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato, la tipologia di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata (es. numero del conto corrente, fido/mutuo, deposito titoli). Trattasi in tutta evidenza di un obbligo estremamente oneroso che le Banche sono state costrette a implementare essendo oggi il Provvedimento a regime dal primo ottobre 2014.

Nel settore delle società di telecomunicazione, invece, è stato introdotto con il d.lgs. 69/2012 il concetto di "violazione dei dati personali" che si sostanzia nella violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico. È stato prescritto quindi che il fornitore di un servizio di comunicazione elettronica accessibile al pubblico debba adottare misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, e debba anche informare i contraenti e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando siffatto rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare. Inoltre, in caso di violazione di dati personali, il fornitore deve comunicare senza indebiti ritardi detta violazione al Garante e quando la violazione di dati rischia di arrecare pregiudizio ai dati personali o alla riservatezza del contraente o di altra persona, il fornitore deve informare anche gli stessi senza ritardo dell'avvenuta violazione. Le misure previste a livello generale dal d.lgs. 69/2012 sono state successivamente dettagliate dal Garante Privacy con il "*Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach*)" del 4 aprile 2013. Il provvedimento in esame ha prescritto che ciascun fornitore identifichi e attribuisca un valore ai differenti dati personali che detiene e ai pericoli cui gli stessi sono esposti, individuando la propria soglia di accettazione dei rischi e fissando le opportune strategie di gestione. Il fornitore è anche tenuto a individuare delle soglie di rischio, ad esempio in base a livello basso, medio e alto, in ragione delle quali deve decidere non solo quali misure adottare per garantire un'idonea protezione dei dati detenuti, ma anche se effettuare la comunicazione al contraente o alle altre persone interessate. Lo stesso provvedimento ha chiarito che "*si tratta di valutazioni sostanzialmente analoghe a quelle che i fornitori, sino al 10 febbraio 2012, erano tenuti ad effettuare ai fini della redazione del Documento programmatico sulla sicurezza, misura minima prevista dalla regola 19 del richiamato Disciplinare tecnico, abrogata dall'art. 45, comma 1, lett. d), del decreto legge 9 febbraio 2012, n. 5 (convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35)".* Il provvedimento, oltre a suggerire alcune misure che vanno ad aggiungersi a quelle prescritte con il provvedimento relativo alla "*Sicurezza dei dati di traffico telefonico e telematico*" del 17 gennaio 2008, nonché con quello relativo alle "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" del 27 novembre 2008, ha introdotto per i fornitori l'obbligo di tenere ed aggiornare un inventario delle violazioni, al fine di consentire al Garante di svolgere il proprio compito di controllo sul rispetto, da

parte dei fornitori medesimi, delle disposizioni in materia di violazione dei dati personali. In tale inventario, i fornitori "*devono inserire tutte (e soltanto) le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate le violazioni, le conseguenze che le stesse hanno avuto e i provvedimenti adottati per porvi rimedio*".

In parallelo a tali previsioni l'Autorità Garante ha emesso una serie di altri provvedimenti e prescrizioni che, sempre in alcuni settori o casistiche specifiche, hanno previsto l'obbligo di raccolta di log (si pensi ad alcune specifiche prescrizioni dettate a seguito di istanza preliminari nel settore del fashion e luxury) o l'invito (non sanzionato in quanto norma di moral suasion) a segnalare le violazioni di dati personali (ad esempio nel settore bancario). Sempre in questa direzione, nel "*Provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di mobile remote payment"* del 22 maggio 2014 *,* che si applica all'offerta da parte di fornitori di reti e servizi di comunicazione elettronica accessibili al pubblico di prodotti e servizi digitali (singoli prodotti o servizi in abbonamento) fruibili dall'utente (titolare di una USIM prepagata o postpagata) tramite smartphone, tablet e PC, attraverso servizi di micropagamento mediante terminale mobile, il Garante ha prescritto ai soggetti coinvolti (operatori, aggregatori e venditori) ulteriori misure, rispetto a quelle previste dal Codice a livello generale, per garantire la confidenzialità dei dati, quali sistemi di autenticazione forte per l'acceso ai dati da parte del personale addetto e procedure di tracciamento degli accessi e delle operazioni effettuate.

Di impatto rilevante per il tema della sicurezza informatica è il recente Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 con il quale l'Autorità Garante è intervenuta per garantire e mantenere alti livelli di sicurezza nell'utilizzo di particolari tipi di dati biometrici, in considerazione della crescente diffusione di dispositivi e, in generale, di tecnologie progettate per la raccolta ed il trattamento dei dati biometrici che consente alle organizzazioni di controllare gli accessi, autenticare gli utenti o sottoscrivere documenti informatici attraverso l'impiego di dati biometrici. Il provvedimento introduce la possibilità di un utilizzo facilitato dei dati biometrici che rientrano nella categoria giudicata dall'Autorità "a basso rischio" consistente nell'esclusione della necessità di presentare una richiesta di verifica preliminare del Garante e di richiedere il consenso degli interessati. La condizione perché tale semplificazione operi è che vengano rispettati i presupposti di legittimità contenuti nel Codice della Privacy e nelle Linee Guida (allegate al provvedimento) e che siano adottate tutte le misure e gli accorgimenti tecnici descritti nel provvedimento in esame. Oggetto di disciplina semplificata sono innanzitutto le aree adibite allo svolgimento di attività aventi carattere di particolare segretezza, ovvero prestate da personale selezionato e impiegato in specifiche attività che comportano la necessità di trattare informazioni riservate e applicazioni critiche, le aree in cui sono conservati oggetti di particolare valore o la cui disponibilità deve essere ristretta a un numero circoscritto di addetti (il loro utilizzo improprio può infatti determinare una grave e concreta situazione di rischio per la salute e l'incolumità degli stessi o di terzi) e le aree preposte alla realizzazione o al controllo di processi produttivi pericolosi che richiedono un accesso selezionato da parte di personale particolarmente esperto e qualificato e l'impiego di apparati e macchinari pericolosi, laddove sia richiesta una particolare destrezza al fine di scongiurare infortuni e danni a cose o persone. Il provvedimento esclude invece dalle modalità semplificate individuate dal Garante per i precedenti casi, i trattamenti che prevedono la realizzazione di archivi biometrici centralizzati, per i quali continuerà ad essere obbligatorio richiedere una verifica preliminare.

Da ultimo merita un cenno una tematica di notevole impatto rispetto alla sicurezza informatica ovvero le possibilità ed i limiti del datore di lavoro rispetto all'utilizzo di strumentazioni informatiche da parte dei dipendenti. Pur non essendo in quest'ultimo periodo intervenute modifiche rilevanti nella

regolamentazione vigente, si rileva come la diffusione dell'utilizzo di tecnologie come la localizzazione geografica, abbia indotto l'Autorità garante a specifiche prese di posizione sul tema.

Occorre innanzitutto premettere come la tematica dei controlli in ambito IT non sia impattata esclusivamente dalla normativa in materia di protezione dei dati personali ma anche dalle norme in materia giuslavoristica, con particolare riferimento allo Statuto dei Lavoratori, che all'articolo 4 vieta l'utilizzo di apparecchiature con la finalità di controllare a distanza l'attività lavorativa (es. l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa) o prescrive particolare cautele (necessità di un preventivo accordo sindacale o autorizzazione della Direzione Territoriale del Lavoro) nei casi nei quali i controlli sono resi necessari da esigenze organizzative o produttive, o sono richiesti per la sicurezza del lavoro, ma consentono indirettamente la possibilità di un controllo a distanza dell'attività lavorativa.

Sotto il profilo della privacy, il provvedimento di riferimento resta quello contenente le "*Linee guida del Garante per posta elettronica e internet*" del 1 marzo 2007, che fornisce indicazioni utilizzabili in generale per tutte le tipologie di controllo in ambito IT. Il Garante per la protezione dei dati personali ha emanato nel mese di aprile 2015 un "*vademecum*" denominato "*Privacy e lavoro*" contenente "*Le regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati,*" nel quale ha sostanzialmente richiamato le principali regole da rispettare nell'ambito dei controlli da parte del datore di lavoro. Senza voler scendere nei dettagli, il documento ribadisce la necessità di rispettare i principi di pertinenza e non eccedenza, di essere trasparenti nei confronti dei lavoratori informandoli non solo delle misure implementate ma anche degli utilizzi consentiti e/o vietati delle strumentazioni informatiche aziendali e delle conseguenze, anche disciplinari, in caso di violazioni. E' necessario inoltre prediligere controlli preventivi che riducano la necessità di raccogliere dati personali dei lavoratori; a titolo esemplificativo, "*Il datore di lavoro per ridurre il rischio di usi impropri di Internet può adottare opportune misure che possono prevenire controlli successivi sul lavoratore, che possono risultare leciti o meno a seconda dei casi e possono comportare il trattamento di dati sensibili, come le convinzioni religiose, filosofiche, politiche, lo stato di salute o la vita sessuale*".

Il sopra citato vademecum del Garante tratta anche la tematica della localizzazione geografica in ragione del fatto che la stessa può essere utile a rafforzare le condizioni di sicurezza dei dipendenti, per esempio, permettendo l'invio mirato di soccorsi in caso di difficoltà. I dati di localizzazione geografica, rilevati da una app attiva sugli smartphone in dotazione ai lavoratori, possono inoltre essere in alcuni casi utilizzati dal Titolare del trattamento purché vengano adottate adeguate cautele a protezione della loro vita privata. In due precedenti provvedimenti legati a istanze di verifica preliminare (*Provvedimento Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Wind Telecomunicazioni s.p.a.* - 9 ottobre 2014; *Provvedimento Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a.* - 11 settembre 2014) il Garante, fermi restando gli obblighi normativi in materia di controllo a distanza dell'attività lavorativa e ritenute legittime le finalità stabilite dalle aziende ai fini dell'utilizzo dei dati di localizzazione geografica, ha tuttavia dettato alcune regole a cui detti trattamenti devono sottostare. In particolare il Garante ha stabilito che:

- non è consentito procedere, di regola, alla rilevazione continuativa dei dati relativi alla localizzazione e è necessario prevedere specifici protocolli che regolamentino i casi nei quali possa

risultare necessario (es. situazioni di emergenza o pericolo per il dipendente), individuando i soggetti legittimati a tale accesso;

- si deve procedere alla sistematica cancellazione delle rilevazioni (es. configurare il sistema perché tratti l'informazione relativa all'ultima posizione inviata dallo smatphone, cancellando quella immediatamente precedente) e dell'ultima rilevazione al termine della giornata lavorativa;
- devono essere adottate specifiche misure idonee a garantire che le informazioni presenti sugli smartphone visibili o utilizzabili dall'applicazione istallata siano riferibili esclusivamente ai dati di localizzazione geografica;
- occorre impedire il trattamento di dati ultronei (es. dati di traffico telefonico, sms, posta elettronica, ecc.);
- si deve configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva anche quando l'applicazione lavora in background
- gli interessati sul trattamento dei dati di localizzazione geografica devono essere informati e posti nella condizione di conoscere finalità e modalità di trattamento (informativa ex art. 13 d.lgs. 196/2003);
- vanno fornite istruzioni ai dipendenti relativamente all'utilizzo del dispositivo, raccomandando altresì di effettuare la pulizia dei dati memorizzati localmente dall'applicazione, fatte salve eventuali esigenze di conservazione da parte del lavoratore.
- è opportuno informare i dipendenti sulle ipotesi in cui è consentita la disattivazione della funzione di localizzazione nel corso dell'orario di lavoro e sulle eventuali conseguenze nel caso in cui la disattivazione avvenga con modalità non consentite;
- i dipendenti devono essere informati sulla possibilità di disattivare la localizzazione al di fuori dell'orario di lavoro.

A conclusione del presente contributo, si rileva come la tematica della sicurezza informatica sia ampiamente disciplinata a livello normativo attraverso le previsioni generali del Codice della Privacy e da numerosi provvedimenti emanati dall'Autorità garante in materia di protezione dei dati personali. Vero quanto detto, c'è da aspettarsi che l'approvazione del Regolamento europeo in materia di privacy sia destinata ad apportare ulteriori modifiche alla tematiche della sicurezza informatica, attraverso l'introduzione di nuovi obblighi e l'aggravamento dei profili di responsabilità. Si ritiene quindi opportuno che le organizzazioni valutino sin d'ora l'impatto che potrebbe avere la nuova regolamentazione sulla propria gestione della sicurezza informatica per non farsi trovare impreparati dalla sua entrata in vigore.

Andrea Reghelin

Andrea Reghelin è senior compliance manager di Partners4Innovation. Dopo una specializzazione in organizzazione d'impresa e tecnologie dell'informazione ed il conseguimento dell'abilitazione alla professione forense, si occupa di compliance aziendale con particolare riferimento al diritto delle nuove tecnologie (privacy, controlli in ambito IT, contratti informatici, ecc.) e alla prevenzione della criminalità d'impresa (d.lgs. 231/2001, sicurezza sul lavoro e ambiente), fornendo supporto consulenziale prevalentemente a organizzazioni di elevata complessità. E' docente a numerosi eventi formativi nelle tematiche di competenza nonché autore di articoli e contributi su riviste specializzate."