secsolution magazine
02·18
www.media.secsolution.com

# Sicurezza privacy e cyber

Collana Monografica

E

## editoriale

# Professionalità vuol dire evoluzione

Secondo IHS Markit la domanda di telecamere professionali per la videosorveglianza – passata da 10 milioni di unità a livello globale nel 2006 ad oltre 100 milioni nel 2016 – continuerà a crescere per tutto il 2018: le previsioni di vendita superano infatti i 130 milioni di unità. L'Italia non fa eccezione: il mercato c'è e si vede, basta guardare il successo delle manifestazioni di settore per comprendere che la sicurezza rappresenta un unicum di eccellenza nello scenario dell'industria elettronica ed elettrotecnica. Certamente il mercato è sempre più inflazionato, il fai da te imperversa anche nel mondo business e diverse figure di altri comparti sono attratte dall'interessante redditività del comparto sicurezza. In questo scenario, differenziarsi è ormai diventato un must. Ma come?

**La crescita professionale è l'elemento primario per intercettare il cambiamento in atto e per sfruttare le opportunità da cogliere**

Noi crediamo che la norma sia la migliore linea guida per muoversi su una base competitiva equa e sicura. Per farlo, occorre però prima formarsi. La crescita professionale è infatti un elemento fondamentale per intercettare il cambiamento in atto e le opportunità da esso derivanti. Oggi si parla tanto di GDPR e dell'impatto che la regolamentazione europea sulla privacy e la protezione del dato potrà avere sul mercato italiano della sicurezza e sorveglianza. C'è chi si trincera dietro allo spauracchio di nuovi limiti e balzelli e c'è invece chi sceglie di entrare nella materia e di metabolizzarla a tal punto da trasformarla in un vantaggio competitivo non solo sul fronte di una produzione compliant by design, ma anche sul fronte consulenziale. Che peraltro oggi può essere certificato e reso quindi immediatamente spendibile. Ma ogni certificazione presuppone un percorso formativo serio ed affidabile. Ecco perché questo numero è incentrato sul GDPR: perché è dalla serietà della formazione che si vede la stoffa professionale di un comparto sul quale noi, per la prima e milionesima volta, ci sentiamo di scommettere.

secsolution magazine 02•18
www.secsolution.com

**Direttore responsabile**
Andrea Sandrolini

**Coordinamento editoriale**
Ilaria Garaffoni
redazione@ethosmedia.it

**Direzione Commerciale**
Roberto Motta
motta@ethosmedia.it

**Ufficio Traffico**
Carolina Pattuelli
pattuelli@ethosmedia.it
tel. +39 051 0475136

**Ufficio estero**
international@ethosmedia.it

**Pubblicità**
Ethos Media Group srl
pubblicita@ethosmedia.it

**Sede Legale**
Via Venini, 37
20127 Milano

**Direzione, redazione, amministrazione**
Ethos Media Group srl
Via Caduti di Amola, 31
40132 Bologna (IT)
tel. +39 051 0475136
Fax +39 039 3305841
www.ethosmedia.it

**Registrazione**
Tribunale di Bologna
n. 8423 del 29/06/2016

**Iscrizione al Roc**
Ethos Media Group s.r.l.
è iscritta al ROC
(Registro Operatori di Comunicazione)
al n. 19315 del 2 marzo 2010

**Periodicità**
Bimestrale

**Privacy (banche dati)**
Le finalità del trattamento dei dati dei destinatari del Periodico consiste nell'assicurare informazioni tecniche e specializzate a soggetti che per la loro attività sono interessati ai temi trattati. Tali dati sono trattati nel rispetto del D.Lgs. 196/2003. Responsabile del trattamento dei dati raccolti in banche dati ad uso redazionale è il direttore responsabile a cui gli interessati potranno rivolgersi per esercitare i diritti previsti dall'art. 7 del D. Lgs. 196/2003

**Marco R. A. Bozzetti**
Presidente AIPSI e CEO di Malabo Srl

# Attacchi digitali: situazione italiana e come contrastarla

Nel suo intervento a Secsolution Forum 2018, Marco Bozzetti, Presidente di AIPSI, l'Associazione Italiana dei Professionisti di Sicurezza Informatica e Capitolo italiano della mondiale ISSA, ha presentato la situazione in Italia sugli attacchi digitali facendo riferimento, tra gli altri, ai dati dei vari Rapporti annuali dell'OAD, Osservatorio Attacchi Digitali in Italia, e poi fornendo alcune indicazioni su come contrastare tali attacchi. Essi dipendono da vulnerabilità tecniche dei sistemi digitali e dalle vulnerabilità comportamentali degli esseri umani che li usano, sia come utenti finali sia come amministratori (ai diversi livelli) degli stessi.

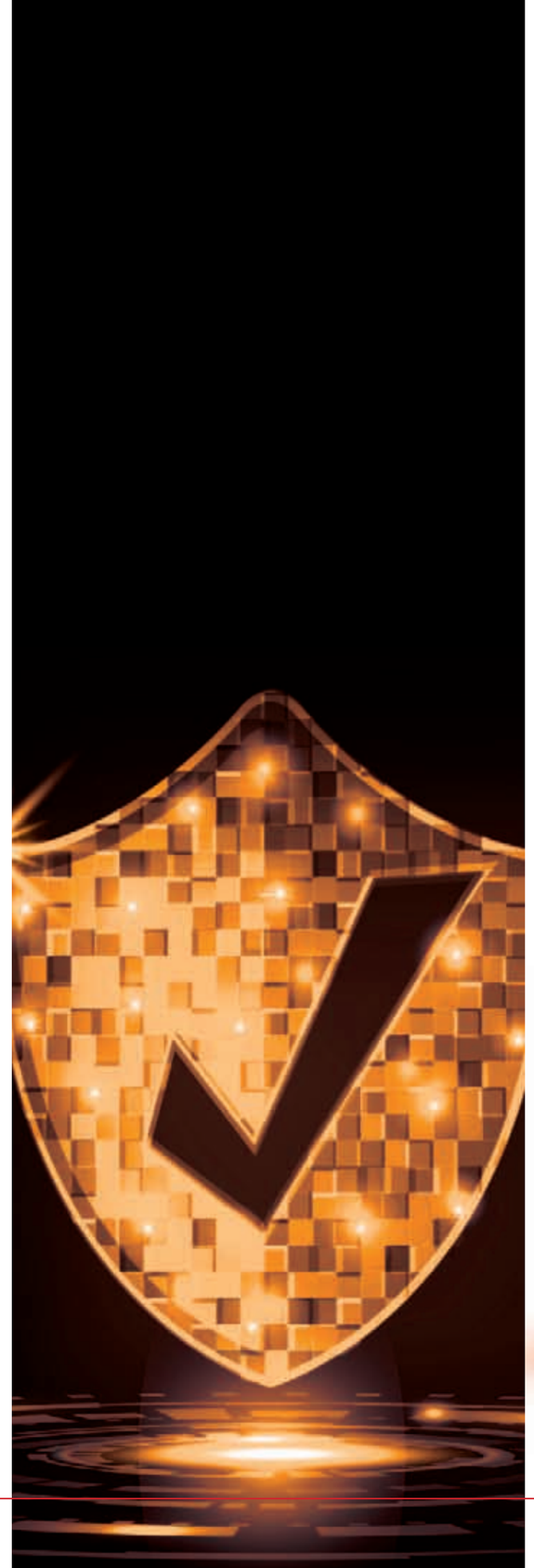
**La sicurezza assoluta non esiste: occorre ridurre rischi ed impatti per garantire un'idonea continuità operativa.**

**Vulnerabilità tecniche**

Molte e di vario tipo le vulnerabilità tecniche: la maggior parte di queste sono note, registrate e catalogate in apposite banche dati, come ad esempio CVE, e presenti in tutti i sistemi operativi, middleware ed applicazioni. Sono normalmente disponibili da parte del fornitore delle correzioni (patch), ma per alcune vulnerabilità non sono state realizzate. Altre vulnerabilità, pur esistendo, non sono state scoperte, e costituiscono, come le precedenti, un possibile e grave punto di attacco.

**Il fattore umano**

Le vulnerabilità maggiori e più critiche sono però costituite dai comportamenti umani, ben più difficili da correggere e da prevenire: ad esempio, per gli amministratori dei sistemi informatici, si parla di errori operativi e ritardi nell'aggiornamento delle release e delle patch, mentre per gli utenti finali ci si riferisce all'uso di password banali, all'apertura di e-mail e relativi allegati di persone ed enti non noti, etc. Le vulnerabilità umane possono poi essere ulteriormente enfatizzate da carenze organizzative, quali la mancanza di controlli e di addestramento, la mancanza di analisi dei rischi e di procedure organizzative sulla sicurezza, e così via.



**Attacchi più diffusi**

I Rapporti OAD degli scorsi anni evidenziavano come le tipologie di attacchi più diffusi in Italia fossero sempre le stesse: malware, social engineering, saturazione delle risorse, furto di dispositivi ICT. Un'anteprima dell'OAD 2018, alla data in corso di realizzazione (il Rapporto OAD 2018 saraà pubblicato a settembre 2018) e che ha introdotto una rigorosa separazione tra che cosa viene attaccato e come, indica provvisoriamente (l'analisi dei dati raccolti è ancora in elaborazione e queste indicazioni potrebbero poi essere, almeno in parte, differenti) che "il cosa" riguarda soprattutto i sistemi terziarizzati, l'identità digitale, le reti ed i DNS. "Il come" è prevalentemente causato da malware e da script.

**Come proteggersi**

In un mondo sempre più automatizzato ed informatizzato, e quindi sempre più vulnerabile con attacchi specifici o di massa, come proteggersi? La sicurezza assoluta non esiste, occorre ridurre rischi ed impatti per garantire l'idonea continuità operativa. La sicurezza digitale non è solo un problema tecnico, è un problema di business e come tale va affrontato dal vertice dell'organizzazione. Per proteggersi occorre analizzare quali sono i reali rischi digitali, e come fare per prevenirli nel contesto della propria realtà culturale, organizzativa e di sistema informatico. Occorre prevenire gli attacchi, e sapere cosa fare quando essi occorrono, per ridurne gli impatti. Le diverse misure di sicurezza da attuare, sia tecniche sia organizzative, debbono essere ben bilanciate: l'attacco colpisce infatti quasi sempre l'anello più debole della catena. E' bene far riferimento agli standard e alle best practice più consolidate a livello mondiale, sia per l'analisi rischi, sia per le misure di sicurezza, oltre che per la loro gestione.

**A chi rivolgersi**

La stragrande maggioranza delle aziende e delle PA italiane sono piccole e piccolissime, e non hanno e non possono avere al loro interno le specifiche competenze in merito. Devono delegare a consulenti e fornitori che non solo abbiano competenze aggiornate, ma che le usino per risolvere efficacemente (ed eticamente) i problemi di sicurezza del cliente, e non per rivendere quello che sanno e/o i prodotti che hanno a magazzino (magari obsoleti … ma il cliente non lo sa). Come fare per scegliere un affidabile e corretto consulente e/o fornitore? Oltre al passaparola, all'autorevolezza ed esperienza che può mostrare ed al "fiuto" del cliente stesso, una condizione necessaria (ma non sufficiente) sono le certificazioni professionali europee per l'ICT, quali eCF (EN 16234 1:2016), e la partecipazione a qualificate associazioni di categoria, quali ad esempio AIPSI. La sicurezza digitale è sicuramente un costo complessivo non indifferente per qualsiasi struttura, privata e pubblica, piccola o grande: ma quale è il costo della non sicurezza?

**Fabrizio Cugia di Sant'Orsola**
Avvocato specializzato in diritto delle comunicazioni elettroniche, IT, privacy e Fintech

# No Data, No Party: la profilazione nel GDPR

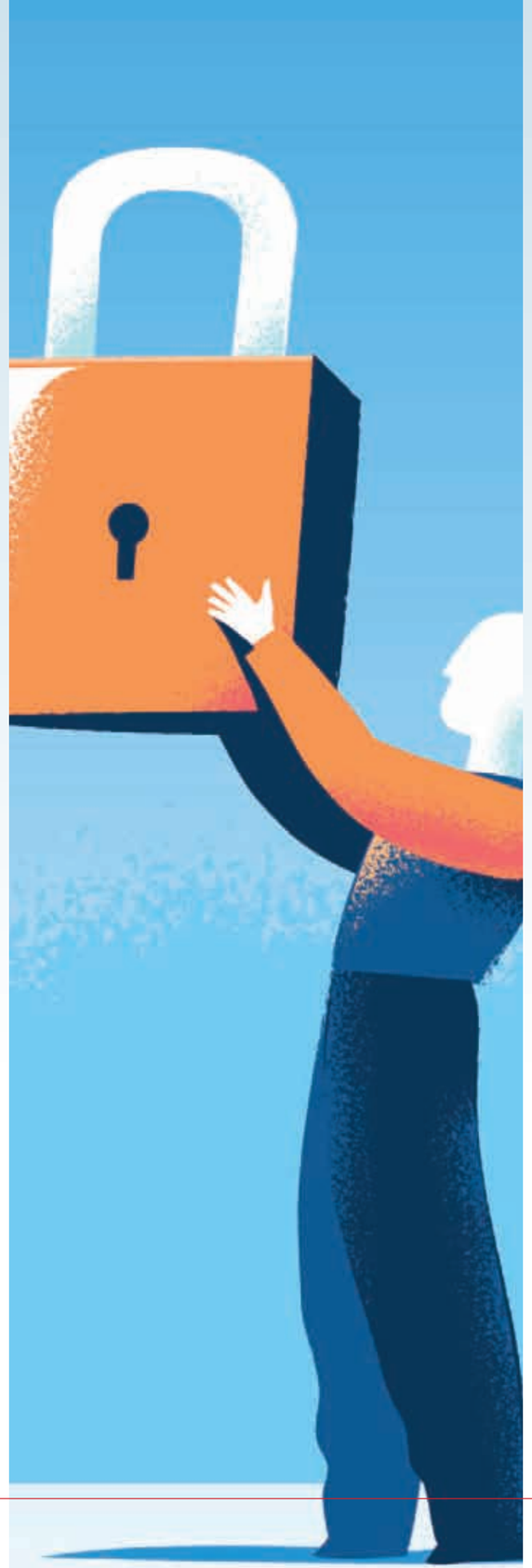
È stato calcolato che nei prossimi dieci anni sul nostro pianeta vi saranno oltre 300 miliardi di device collegati in Rete, molti dei quali interattivi e capaci di interrogare i big data in via autonoma e diretta ed atti a rilevare dati inerenti ai comportamenti umani tramite uso di traccianti o sensori di geolocalizzazione. Il GDPR interviene anche sul fenomeno dell'uso e trattamento automatizzato di dati, ponendo nuovi obblighi a carico dei titolari del trattamento per l'uso di sistemi, apparati o tecnologie che non consentono per loro stessa natura la minimizzazione dei dati, obbligo generale posto dal GDPR a carico di ogni titolare del trattamento.

**Il GDPR**

Come noto, il diritto alla privacy è un diritto fondamentale sancito assai prima del GDPR. L'art. 7 della Carta fondamentale dei diritti UE stabilisce che ogni persona ha diritto al rispetto della propria vita privata e del proprio consesso famigliare, oltreché del proprio domicilio e delle proprie comunicazioni. Dal canto loro gli artt. 8 e 16 della Carta stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano, ed il tema regolamentare è come conciliare questi diritti inalienabili e personali con l'evoluzione tecnologica sempre più invasiva e permeata nei sistemi produttivi contemporanei. Il GDPR rappresenta in tal senso una visione evoluta della responsabilizzazione dei titolari del trattamento, incentrata sul tema dell'accountability e della responsabilità oggettiva dei titolari nella corretta previsione dei rischi privacy oggetto di attività di mappatura. In tal senso il privacy by design e by default costituiscono indubbi caposaldi dell'attività di prevenzione generale posta a carico di ogni titolare. Tuttavia appare legittimo chiedersi se proprio la profilazione dei dati, ossia la gestione automatizzata di dati personali, non costituisca il vero e proprio banco di prova dell'efficacia del GDPR, innanzitutto con riguardo all'interazione con i big data nell'offerta di servizi IoT (internet of things) e M2M.

**Profilazione: banco di prova**

Le misure privacy rischiano infatti di risultare di difficile applicazione ed efficacia nel particolare quadro della parcellizzazione dei ruoli e delle intermediazioni e disintermediazioni proprie dell'evoluzione tecnologia ed economica (si pensi all'intermediazione nei pagamenti, dove i ruoli dei gestori nel trattamento dei dati possono oscillare considerevolmente tra gli operatori della filiera, tra istituti bancari, operatori tlc e service providers nella sola transazione di acquisto fatta tramite device con riconoscimento biometrico). Nei settori bancari, sanitari, assicurativi e pubblicitari già oggi l'interazione ed uso dei dati personali scambiati tra soggetto interessato proprietario dei dati e provider di servizi (si pensi alle assicurazioni "black box") permettono non soltanto di scegliere profili di consumo e contrattazioni specifiche per tipologia di consumer, ma più ancora di garantire il continuo rispetto di tali condizioni parametrate proprio al comportamento del singolo, rilevato di continuo dai dispositivi-sensori interattivi con le centrali del titolare del trattamento dati (nel caso di specie, società di assicurazioni). Il progresso tecnologico ha reso tali trattamenti maggiormente efficienti ed economici, ponendo tuttavia un particolare carico di rischi per i diritti e le libertà degli individui connessi al loro utilizzo. I processi decisionali automatizzati sono inoltre spesso basati su algoritmi complessi, spesso sconosciuti o comunque incomprensibili agli individui, propri dell'intelligenza artificiale, che a sua volta (al suo interno)



contempla una pletora di applicazioni e servizi anche dissimili. Ciò che li accomuna è il "dare" alla macchina un problema ed insegnare alla stessa come risolverlo per proprio conto, tuttavia il "pattern" di ragionamento empirico per giungere alla definizione di soluzioni alternative è "programmato" in modalità anche sostanzialmente diversa.

**Behavioral advertising**

Il behavioral advertising (pubblicità comportamentale) è un esempio di attività di profilazione "generata" da dati prodotti dai comportamenti dei soggetti interessati. I sensori traccianti elaborano sui gusti, tendenze, acquisti, programmi di appartenenza, interazioni, ecc., per individuare il comportamento umano e circoscriverlo (ossia circoscrivere i soggetti interessati) in "cluster" di appartenenza. La finalità della profilazione è una tecnica in stretta connessione funzionale al concetto di identificazione/identificabilità della persona. La problematicità del processo di profilazione risiede soprattutto nel fatto che risulta essere invisibile agli interessati, ed il produttore o operatore di apparati IoT connessi è anche il titolare dei dati processati da tale apparato. In caso di attacchi cyber, il produttore/operatore/titolare potrà quindi essere responsabile sotto due profili: privacy e come produttore dell'apparato, ed occorrerà analizzare la complessità e le caratteristiche di sicurezza adottate nel prodotto.

**Profilazione**

Per profilazione si intende una "tecnica di trattamento automatico mediante algoritmi di molteplici tipologie di dati personali relativi a quantità numericamente elevatissime di persone, per attribuire a ciascuna di queste ultime un profilo, ovvero una categoria predefinita e delineata attraverso parametri che il responsabile del trattamento considera necessari alla sua ricerca, al raggiungimento del suo scopo; il target è studiato nelle sue abitudini di consumo e negli stili di vita che ne rivelano attitudine e capacità di spesa, gusti per alcuni prodotti o servizi e disinteresse per altri, caratteristiche legate alla sua identità personale" (Pacileo). La profilazione, pertanto, si compone di tre elementi base: il trattamento deve essere svolto in forma automatizzata, esso deve essere condotto su dati personali e deve perseguire il suo obiettivo studiando il comportamento delle persone fisiche.

**La tutela del GDPR**

Secondo il GDPR, l'interessato deve poter non sottostare inconsapevolmente al trattamento dei dati mediante profilazione (ed in generale tutti i processi automatici). Ciò è confermato dallo stesso Regolamento all'art. 22 GDPR. Secondo la norma, quando il processo decisionale è automatizzato, l'interessato ha il diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato (compresa la profilazione, che costituisce una delle forme di trattamento automatizzato), che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Ciò pone l'obbligo a carico dei titolari di ottenere il previo consenso esplicito, a meno che non vi siano esigenze o prestazioni contrattuali o il trattamento sia autorizzato dal diritto nazionale o dell'UE. Nella precedente disciplina privacy, il sistema prevedeva "sanzioni" contro comportamenti contrari agli obblighi, e non sussisteva tra le eccezioni il consenso reso dall'interessato.

**Accountability**

Diverso ruolo, come visto, è rivestito dall'accountability, con l'obbligo di valutazione preventiva. Il problema legale riguarda quindi, innanzitutto, il consenso espresso dal soggetto interessato, ed in particolare il rapporto tra consenso, legittimi interessi e adempimenti contrattuali. Il consenso nell'area dell'AI e della stessa profilazione è difficilmente definibile a priori, stante l'evoluzione dei dati "processati" e generati a getto continuo dagli apparati. Giustificare il trattamento di tali dati dal punto di vista contrattuale - come adempimento di prestazioni richieste - determina un margine molto ristretto mirato ad una prestazione "cristallizzata" nel tempo, ossia non dinamica. Così, parte della soluzione pare risiedere sul concetto di "interesse legittimo" in capo al Titolare del trattamento, interesse che non è sufficiente quando si tratta di speciali categorie di dati (es. salute, biometrici, ecc.) proprio di particolare rilievo nell'AI. Il legittimo interesse pone l'onere a carico di chi intende sviluppare i dati di dimostrare che tale sviluppo non pone un carico intollerabile ai diritti sulla privacy. Si tratta, quindi, di un esercizio di accurato bilanciamento e contemperamento, i cui corretti confini sono tutti ancora da individuare.

**Rocco De Nicola,** Professore presso IMT Alti Studi Lucca
**e Paolo Prinetto,** Professore presso il Politecnico di Torino

# Un libro Bianco sulla Cybersecurity in Italia

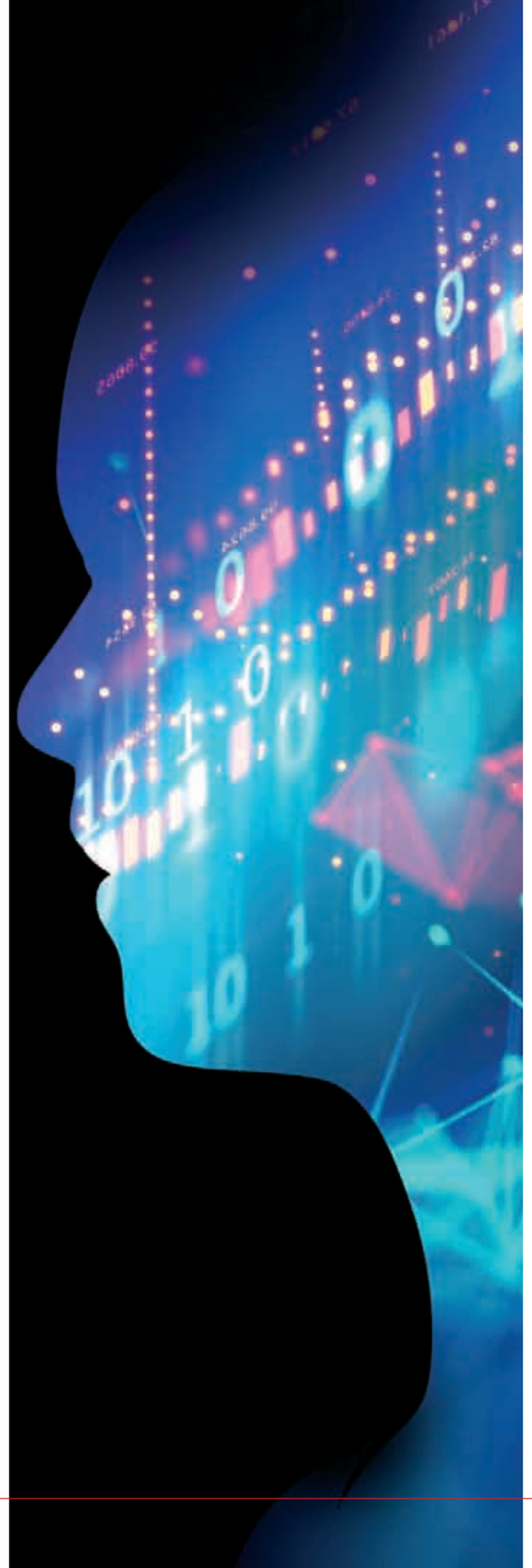
In un mondo sempre più digitalizzato, gli attacchi informatici suscitano allarme nella popolazione, causano danni ingenti all'economia e mettono in pericolo la stessa incolumità dei cittadini quando colpiscono reti di distribuzione di servizi essenziali come la sanità, l'energia, i trasporti, vale a dire le infrastrutture critiche della società moderna. Si immagini cosa potrebbe succedere se si spegnessero all'improvviso tutti i semafori di una metropoli, se si bloccassero gli ascensori e le ambulanze non potessero più ricevere l'indirizzo giusto per recuperare i feriti. Inoltre, un attacco informatico di successo potrebbe anche rappresentare un momento di non ritorno per la credibilità di un'azienda, lo sviluppo del suo business e la capacità di vendere prodotti in un regime di sana concorrenza. Ugualmente, un attacco informatico riuscito potrebbe destabilizzare il mercato azionario facendo sprofondare interi paesi nel caos, oppure bloccare i rifornimenti di gas in inverno o il ciclo dei rifiuti urbani; il conseguente scenario politico sarebbe drammatico.

**Sicurezza fisica e logica**

Gli strumenti di protezione per la sicurezza fisica, per il rilevamento delle intrusioni, per il controllo del territorio dipendono sempre di più dagli strumenti informatici. Come accennato sopra, attacchi informatici possono bloccare o anche distruggere sistemi fisici, ma è anche vero che sistemi per garantire la sicurezza fisica possono essere utilizzati per attacchi informatici. I cybercriminali possono sfruttare le nostre telecamere di casa per sapere tutto di noi. Si legge sempre più spesso di attacchi a sistemi di sicurezza informatici portati a termine tramite delle "botnet" formate da milioni di dispositivi, per la maggior parte videocamere, connessi a internet, dei quali i criminali avevano preso precedentemente il controllo. Le videocamere e altri dispositivi non sicuri vengono utilizzati dagli attaccanti per fare continue richieste ai siti obiettivo, in numero tale che lo portano al collasso (DDOS - Distributed Denial of Service Attack). Quindi sicurezza fisica e sicurezza cibernetica saranno sempre più connesse.

**IoT e altri rischi**

Altri attacchi sono portati avanti con successo sfruttando dispositivi IoT presenti in giocattoli, in distributori automatici di bevande e in interruttori intelligenti per la domotica. I dispositivi connessi alla rete che ci fanno parlare di Internet of Things (IoT) trovano ormai impiego nelle situazioni più disparate che includono, tra l'altro, dispositivi mobili (smartphone e tablet), casa e applicazioni domotiche, sensori e attuatori in ambito industriale, trasporti (dall'automotive al ferroviario, dalla cantieristica all'aeronautica e ai droni), infrastrutture critiche e Cyber Physical System (sistemi di monitoraggio e controllo). Le stime più recenti parlano di circa 6 miliardi di dispositivi connessi a Internet nel 2017, con una previsione di crescita a 21 miliardi nel 2020.



La diffusione di dispositivi IoT e dei nuovi servizi da loro resi disponibili ha accresciuto a dismisura la cosiddetta "superficie di attacco", introducendo di fatto nuove vulnerabilità. Molte applicazioni, infatti, abilitate dagli scenari IoT, aprono la porta a vulnerabilità totalmente nuove e largamente inesplorate, che possono esporre gli utenti a effetti particolarmente seri, se non prevenuti e trattati in modo specifico. Questo fenomeno è oggi particolarmente sentito anche in ambito industriale dove, grazie anche agli incentivi resi disponibili dai vari piani di sviluppo di Impresa 4.0, la diffusione di dispositivi IoT ha raggiunto livelli molto significativi. Occorre poi evidenziare come la scoperta e la pubblicizzazione di una vulnerabilità in un dispositivo IoT si traduca, immediatamente e contemporaneamente, in una vulnerabilità per tutte le apparecchiature e tutti i sistemi in cui quel dispositivo è impiegato. È fondamentale pertanto che tutti gli attori operanti all'interno dell'area della sicurezza siano coscienti dei rischi associati al "sempre connessi e ovunque".

**Libro Bianco sulle sfide di cybersecurity**

Alla fine del 2015, il Laboratorio Nazionale di Cybersecurity del CINI ha realizzato un Libro Bianco per raccontare le principali sfide di cybersecurity che il nostro Paese doveva affrontare nei cinque anni successivi. Il volume si concentrava soprattutto sui rischi derivanti dagli attacchi cyber e delineava alcune raccomandazioni anche organizzative. Ne 2018 abbiamo prodotto un nuovo volume nato come continuazione del precedente, con l'obiettivo di delineare un insieme di ambiti progettuali e di azioni trasversali che la comunità nazionale della ricerca ritiene essenziali.
Ambiti e azioni contengono tipicamente vari progetti operativi rivolti sia al settore pubblico sia a quello privato. Ciascuna presentazione include le motivazioni, un breve stato dell'arte, e un insieme di sfide da affrontare e di obiettivi da perseguire. I diversi ambiti progettuali sono stati raccolti in cinque aree operative:

- *Infrastrutture e Centri* - In quest'area vengono considerati gli strumenti e le azioni necessarie a mettere in sicurezza la rete Internet nazionale e i data center della PA; vengono inoltre presentate alcune tipologie di centri di competenza da attivare sul territorio nazionale per rafforzare le difese del sistema Paese.

- *Azioni abilitanti* - In quest'area vengono considerate le azioni necessarie a rendere più sicuro il ciclo di gestione della minaccia: dalla protezione di applicazioni critiche nazionali alla creazione di una banca nazionale delle minacce, dalla difesa da attacchi diversi (cibernetici, sociali, fisici) all'analisi forense, dalla gestione del rischio a livello sistemico alla protezione attiva.

- *Tecnologie abilitanti* - Gli ambiti progettuali in quest'area mirano a irrobustire alcune delle tecnologie di base da utilizzare per proteggere dati, limitare attacchi e loro effetti e, in generale, per aumentare la resilienza dei sistemi anche attraverso soluzioni mirate a "security by design". In particolare vengono considerate architetture hardware che garantiscano livelli più alti di sicurezza, crittografia, blockchain, tecnologie biometriche e quantistiche.

- *Tecnologie da proteggere* - In quest'area vengono presentati gli strumenti e le azioni necessarie a proteggere alcune tecnologie chiave, quali comunicazioni wireless, servizi cloud, logiche funzionali dei sistemi e, anche nella prospettiva di Impresa 4.0, IoT, sistemi di controllo industriale e robot.

- *Azioni orizzontali* - Gli ambiti progettuali relativi a quest'area mirano a garantire la protezione dei dati personali, a innalzare il livello di conoscenza e competenza attraverso progetti di formazione, sensibilizzazione e certificazione e a migliorare la gestione del rischio a livello aziendale.

La lettura del nuovo libro bianco non richiede particolari conoscenze tecniche; il testo è fruibile da chiunque utilizzi strumenti informatici o navighi in rete. Il file .pdf della versione italiana è scaricabile dal sito:
https://www.consorzio-cini.it/images/Libro-Bianco-2018.pdf
mentre una versione in lingua inglese è scaricabile dal sito:
https://www.consorzio-cini.it/images/Libro-Bianco-2018-en.pdf

**Alberto Delaini**
CEO di Delaini & Partners

# Il tuo ERP è già adeguato al GDPR?

Una decina di anni fa le soluzioni applicative utilizzate dalle imprese italiane in pratica non contenevano i dati personali, ma solo quelli aziendali. Più recentemente, sulla spinta dell'esigenza di personalizzare il rapporto tra cliente e fornitore, il collegamento non è più azienda-azienda, ma è diventato in molti casi persona-persona. Prima conseguenza: sia l'ERP – la trave portante della gestione dei processi, sia in misura ancora maggiore il CRM si sono arricchiti di tantissime informazioni che ricadono nella sfera di cui oggi si occupa il GDPR. Citiamo solo ERP e CRM ma sono parecchie altre le soluzioni (pensiamo alla gestione del personale o alla sales force automation) che si trovano a gestire una massa significativa di dati personali e talora anche sensibili.

**L'adeguamento non è un processo immediato**

Chi pensa di usare la bacchetta magica (un software, un consulente, una gestione documentale …) per diventare immediatamente "compliant" sbaglia di grosso. Serve un lavoro metodico e complesso per realizzare una serie di obiettivi:

- sistemare gli aspetti formali (registro dei trattamenti, lettere di incarico, etc);
- sensibilizzare e formare i dipendenti e collaboratori;
- riprogettare alcuni processi che con il GDPR sono diventati critici per la privacy;
- "mettere in sicurezza" i dati personali presenti nel proprio sistema informativo, in modo da poter adempiere a qualsiasi richiesta di variazione o cancellazione, dimostrando formalmente ciò che è stato fatto.

**Le aziende informatiche e il GDPR**

Le strutture che si occupano di software applicativo, tra l'altro, quando decidono di mettersi in regola si trovano di fronte a complicazioni aggiuntive rispetto a quelle di una azienda "normale", ossia:

- quasi sempre sono collegate on line con i propri clienti e hanno accesso ai dati di questi, ad esempio per garantire la manutenzione software remota;
- a volte ospitano fisicamente dati di clienti cui fanno servizio, come nel caso di applicazioni Cloud;
- può accadere che lavorino con elaboratori che ospitano i dati in Paesi Terzi, magari fuori dalla CEE: basti pensare alle soluzioni di e-commerce ospitate su piattaforme quali Amazon.

**Un "decalogo" … in otto punti**

Il GDPR, come tutti gli adempimenti formali, a leggerlo fa girare la testa per la complicazione. In realtà, la cosa più importante è mettersi in testa uno schema da seguire nella fase di adeguamento.
Abbiamo indicato otto requisiti chiave sui quali focalizare l'attenzione:

1. fare l'analisi dei rischi, per capire dove intervenire e con quali priorità;
2. ragionare sui dati e sulla loro vita, perché se non sappiamo dove si trovano (inclusi backup e copie varie di servizio) non potremo mai tenerli sotto controllo né gestirli correttamente;
3. progettare accuratamente le autorizzazioni agli accessi, dato che non è più accettabile un regime di "anarchia" sistematica e incontrollata;
4. impostare e tenere aggiornato il Registro dei Trattamenti, cosa non del tutto semplice;
5. assicurarsi un DPO esperto, perché in ogni adempimento normativo gli aspetti formali contano quasi quanto quelli sostanziali;
6. attrezzarsi per intervenire subito in caso di violazione (data breach);
7. verificare la compliance del proprio sito, che è forse la cosa più facile ma alla quale si pensa poco o niente (politica della privacy etc.);
8. e infine, per il futuro anzi da ieri visto che il 25 maggio è già dietro le spalle, attenzione ad impostare le logiche di Privacy by Design in tutto lo sviluppo del software.





**Giulio Iucci**
Presidente di ANIE Sicurezza

# Convergenza tecnologica: imparare dalle criticità

**Parola d'ordine: Convergenza**

*Convergenza,* in primo luogo tra sicurezza fisica e sicurezza logica dove, oggi, la digitalizzazione rende possibile l'interoperabilità tra i sistemi. Il progredire delle nuove tecnologie ci pone infatti di fronte alla nuova sfida di saper creare soluzioni in cui possano coesistere e collaborare settori differenti e non necessariamente affini tra loro: security, safety e automazione.

**Early Warning**

Apparati e singoli sottosistemi sono, infatti, connessi tra loro, e in alcuni casi anche con le persone, costantemente e in tempo reale, come parte di un unico grande "ingranaggio" che può essere violato, non solo nelle sue infrastrutture critiche ma, più profondamente in ciascuna sua componente, fino ad arrivare all'obiettivo principale. Diventa quindi imprescindibile concepire sistemi di sicurezza non più con un approccio azione-reazione, ma come un'unica "dimensione" che consenta la supervisione - in ottica di quello che viene definito Early Warning - dell'intero ingranaggio.

**Imparare dalle criticità**

Oggi diventa fondamentale imparare dalle criticità generate dalla convergenza tecnologica, così da poterne utilizzare tutti i vantaggi, minimizzando i rischi, attraverso l'adozione di misure tecnologiche, architetturali e procedurali, coerenti e proporzionate al contesto e al bene da proteggere, sia esso materiale, immateriale o umano.

**Analisi del rischio**

Le regole di base di misurazione del rischio rimangono invariate e continuano ad utilizzare i medesimi parametri macro di riferimento per definire le probabilità e l'entità di ciò che può verificarsi. In quest'ottica è fondamentale effettuare a monte e con chiarezza l'analisi del contesto così da definire dettagliatamente quali siano i beni da proteggere e gli eventuali offender. Questo per generare equilibrio e sostenibilità ad un'azione di protezione e prevenzione che sia coerente con i reali rischi e le possibili conseguenze di un'azione criminosa

**Una nuova dimensione**

Il concetto di sicurezza assume una dimensione nuova dove tutti i sistemi connessi, anche residuali, devono essere considerati potenzialmente critici e sensibili e quindi da mettere in sicurezza. Per questa ragione, è necessario determinare quali siano le nuove vulnerabilità introdotte per essere in grado di proteggere ciascun elemento facente parte del sistema, tanto quanto i canali di comunicazione che li uniscono.

**Domenico Laforenza**
Direttore dell'Istituto di Informatica e Telematica del CNR

# La privacy nell'era dell'IoT e dei Big Data

Il paradigma dell'Internet of Things (IoT) (Internet delle "cose" o degli "oggetti") riguarda l'interconnessione, mediante Internet, di miliardi di oggetti intelligenti che ci circondano, ciascuno identificabile e indirizzabile univocamente, in grado di raccogliere, memorizzare, elaborare e comunicare informazioni su se stessi e sul loro ambiente circostante. Questo paradigma, che integra nella rete entità fisiche che fanno parte del mondo reale, rappresenta dunque un'evoluzione di Internet e consente la realizzazione di molte nuove applicazioni e servizi (ad esempio, case e città "intelligenti", trasporti più efficienti, razionalizzazione dei consumi energetici, ecc.) in grado di migliorare la vita quotidiana delle persone e di contribuire anche a generare valore mediante la creazione di nuove imprese. Oggi la principale applicazione di quello che potremmo definire l'Internet "tradizionale" è il Web, nel quale l'intervento umano è ancora predominante, ad esempio per: cercare informazioni tramite un motore di ricerca, fare acquisti, interagire nei social media.
Nel mondo IoT, invece, i sensori sono in grado di operare nella quasi totale autonomia.

**IoT e sensori**
L'uso di sensori (di varia natura, dimensione, complessità e costo) in grado raccogliere, analizzare e trasmettere enormi quantità di dati (inclusi quelli relativi al comportamento delle persone), nonché il successivo sfruttamento di queste informazioni, rende possibile una sempre più accurata profilazione degli individui al fine, ad esempio, di proporre loro prodotti e servizi personalizzati, garantendo nel contempo, alle aziende proponenti, maggiori efficienze nella produzione e commercializzazione. Occorre però dire che, sebbene la prospettiva dell'adozione di sistemi IoT sia molto interessante e promettente, i rischi legati all'uso e sfruttamento indiscriminato dei Big Data sollevano anche molti interrogativi e concrete preoccupazioni (alcune delle quali veramente inquietanti) a riguardo di come, e da chi, questi enormi giacimenti di dati sono utilizzati.

**Rischio privacy**
Una delle preoccupazioni più ricorrenti riguarda la tutela della privacy delle persone, visto che, nel caso di Big Data, le tecniche di "anonimizzazione" dei dati, usate comunemente al fine di renderne i soggetti non riconoscibili, possono essere aggirate e rese vane abbastanza facilmente, incrociando opportunamente i tanti e variegati dati raccolti sulle persone, e analizzandoli con sofisticate tecniche di Big Data Analytics. Ne deriva che, di fatto, è possibile identificare le persone e profilarle a svariati livelli di dettaglio, con il serio rischio concreto di "sapere tutto su tutti" e, conseguentemente, aprire varchi nei confronti della privacy e delle libertà delle persone.
Dare una risposta ai tanti quesiti e alle giuste preoccupazioni sulla privacy delle persone, derivanti dall'adozione dei sistemi IoT, è importante anche in una prospettiva di mercato di queste tecnologie, la cui crescita potrebbe essere rallentata dalla mancanza di fiducia da parte dei consumatori.





**Stefano Manzelli**
Consulente enti locali e forze dell'ordine


# Videosorveglianza integrata: bivio privacy tra polizia locale e FFOO

Con l'entrata in vigore della riforma europea sul trattamento dei dati personali, la prima valutazione strategica da adottare in materia di videosorveglianza urbana integrata riguarda l'impatto privacy, ovvero se l'impianto che stiamo progettando sarà utilizzato per prevalenti finalità di sicurezza urbana. Oppure se si tratta di una infrastruttura che sarà dedicata prioritariamente alle attività delle forze di polizia dello stato – come per esempio in caso di impianto comunale di lettura targhe collegato alla banca dati dei veicoli rubati con server dedicato in questura.

**Trattamento dati ad uso polizia**
La profonda differenziazione in materia di trattamento dei dati personali per uso polizia locale ed uso polizia di stato e carabinieri è stata infatti evidenziata dal dlgs 18 maggio 2018, n. 51, che dall'8 giugno scorso ha recepito nell'ordinamento la direttiva Ue 680/2016, specificamente dedicata al trattamento dei dati per finalità di prevenzione, accertamento e perseguimento dei reati o esecuzione di sanzioni penali.
Da una parte dunque il Gdpr, ovvero il regolamento Ue 679/2016 che in qualche modo dovrà portare ad una nuova regolamentazione di dettaglio anche il trattamento dei dati personali attraverso gli impianti di videosorveglianza urbana, con un inevitabile aggiornamento del provvedimento generale del Garante dell'8 aprile 2010.
Dall'altra parte la direttiva 680/2016 che andrà a disciplinare, con la successiva adozione di un regolamento ad hoc, anche la particolarità del trattamento dei dati attraverso i sistemi di videosorveglianza urbana per finalità interforze.

**Cambia il dettaglio operativo**
I principi introdotti dal regolamento 679 e dalla direttiva 680 sono molto simili. Quello che cambia sostanzialmente sarà il dettaglio operativo. L'esempio più efficace riguarda il tempo massimo di conservazione delle immagini. Se si tratta di un impianto tradizionale di lettura targhe dei veicoli in transito per finalità sanzionatorie, stradali e di sicurezza urbana, il periodo di conservazione resterà invariato: 7 giorni. Se l'impianto sarà stato invece progettato in origine per una prevalente finalità di polizia di stato, con server posizionato in questura per il match con la banca dati dei veicoli rubati, il tempo massimo di conservazione dei dati non potrà essere inferiore a 60 giorni. Un lasso temporale necessario per attività investigative spesso lunghe e complesse. In pratica la disciplina della direttiva n. 680/2016 è necessariamente più permissiva al fine di non contrastare l'attività degli organi inquirenti. Ma sarà un decreto ad hoc a dover entrare nel dettaglio di queste opportunità investigative. Spetterà infatti al regolamento che dovrà essere adottato ai sensi dell'art. 5 del dlgs 51/2018, individuare, tra l'altro, "le modalità di conservazione dei dati, i soggetti legittimati ad accedervi, le condizioni di accesso, le modalità di consultazione, nonché le modalità e le condizioni per l'esercizio dei diritti".

**Nelle more**
Senza i dettagli operativi che verranno individuati da questo regolamento, il rischio è progettare impianti di videosorveglianza urbana che potrebbero risultare non idonei ad un uso interforze. Ovvero di impianti progettati nel rispetto di improbabili regole tecniche non congruenti con le aspirazioni tecnologiche ed informative del Centro elettronico nazionale del Ministero dell'interno.
E quindi neppure convergenti con il rispetto delle diverse competenze degli organi di polizia locale e dello stato e delle relative differenziazioni in materia di trattamento dei dati personali.

**Roberta Rapicavoli**
Avvocato esperto in Information Technology e privacy e Docente Ethos

# Dalla verifica preliminare alla valutazione d'impatto: cosa cambia per la TVCC?

Alcuni trattamenti possono presentare dei rischi per i diritti e le libertà dell'interessato. Prima del loro avvio, si rende pertanto necessaria un'attenta valutazione, tesa ad individuare le misure e gli accorgimenti necessari per assicurare le adeguate garanzie. Fino al 25 maggio 2018 tale valutazione era rimessa all'Autorità Garante, nell'ambito di una verifica preliminare, effettuata anche a seguito di un interpello del titolare (si veda l'art. 17 del Codice privacy).

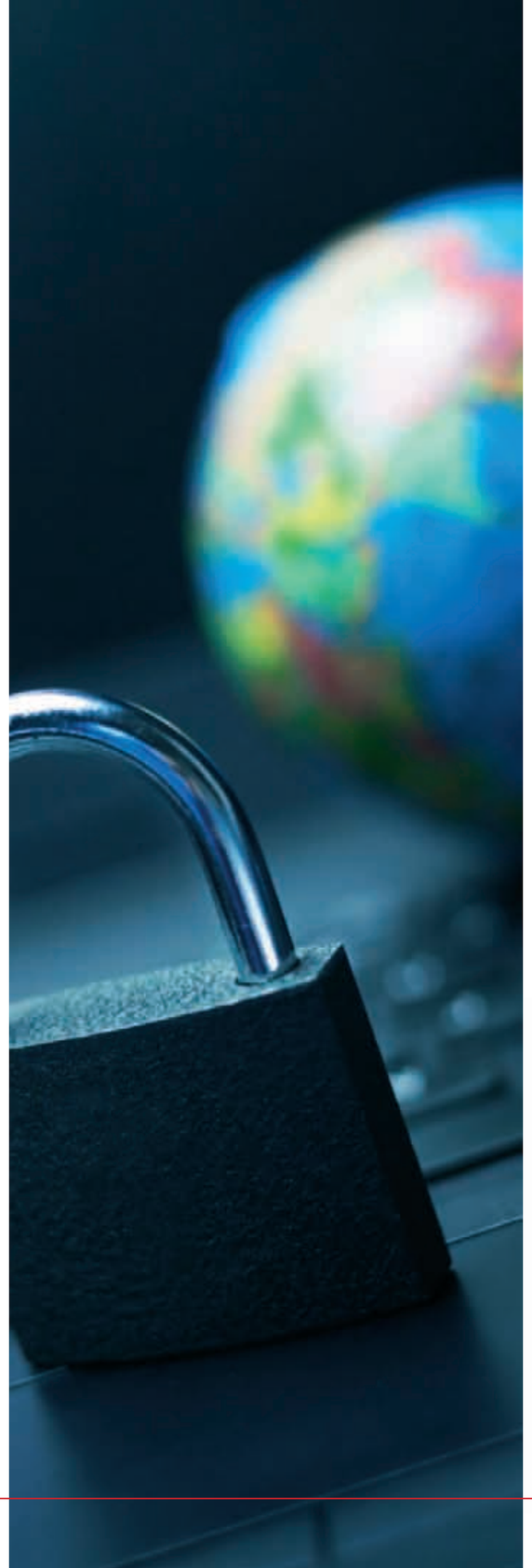
**Spetta al Titolare**

Il Regolamento UE 2016/679 (Regolamento Generale sulla Protezione dei Dati, noto anche come RGPD), non ripropone l'obbligo di verifica preliminare al Garante. Spetta infatti adesso direttamente al Titolare, in base al principio di responsabilizzazione o accountability, esaminare, fin dalla fase di pianificazione e progettazione, i profili legati al trattamento dei dati e, nel caso di rischi elevati, effettuare la valutazione d'impatto prevista dall'art. 35 del nuovo Regolamento, rimanendo il coinvolgimento dell'Autorità limitato alle sole ipotesi in cui, all'esito della valutazione, non si riuscissero a trovare misure sufficienti per ridurre i rischi a un livello accettabile.

**Se dall'analisi emergono rischi elevati, deve essere effettuata una valutazione di impatto**

**Rischio elevato o no?**

Come capire se il trattamento presenta o meno un rischio elevato e, quindi, comprendere se dover effettuare o meno una valutazione di impatto? Oltre ai casi indicati nello stesso art. 35 del RGDP (tra cui rientra la sorveglianza sistematica su larga scala di una zona accessibile al pubblico), e in attesa che l'Autorità Garante predisponga e renda pubblico l'elenco delle tipologie di trattamenti soggetti alla valutazione di impatto, per verificare se il trattamento da avviare presenti o meno un rischio elevato, devono essere considerati la natura, l'oggetto, il contesto e le finalità del trattamento e la sussistenza o meno di due o più dei criteri richiamati dal Gruppo dei Garanti europei nelle Linee Guida in materia di valutazione di impatto (tra cui rientrano, tra gli altri, l'uso innovativo o l'applicazione di nuove soluzioni tecnologiche od organizzative, i dati relativi a interessati vulnerabili, il monitoraggio sistematico e il trattamento su larga scala).



**Valutazione d'impatto**

Se dall'analisi dei citati aspetti legati al trattamento da avviare emergono rischi elevati, deve essere effettuata una valutazione di impatto, che deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati; e
- le misure previste per affrontare i rischi.

Nel caso in cui, all'esito della valutazione, dovessero residuare dei rischi elevati perché non si riescono a trovare misure sufficienti per ridurre i rischi a un livello accettabile, il titolare si rivolgerà all'Autorità Garante. L'autorità non avrà però il compito di "autorizzare" il trattamento, ma di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58 del RGDP (dall'ammonimento fino alla limitazione o al divieto di procedere al trattamento).

**Quali trattamenti**

Il Garante privacy, nel suo provvedimento in materia di videosorveglianza dell'8 aprile del 2010, richiama come trattamenti che presentano dei rischi specifici, da sottoporre a verifica preliminare, quei trattamenti legati a:

- sistemi di videosorveglianza dotati di software che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali;
- sistemi intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli;
- sistemi integrati di videosorveglianza, nei casi in cui le relative modalità di trattamento non corrispondano a quelle individuate nel citato provvedimento;
- allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di sette giorni derivante da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.

Considerando che l'istituto della verifica preliminare, prevista dall'art. 17 del Codice privacy, è venuto meno, in attesa di un elenco in cui siano definite le ipotesi in cui la valutazione sia necessaria, si ritiene che debba continuarsi a prestare attenzione all'impiego dei sistemi di videosorveglianza che il Garante, nel suo provvedimento del 2010, fa rientrare nelle ipotesi di trattamenti rischiosi – effettuando, in tali casi, una valutazione di impatto ai sensi dell'art. 35 del Regolamento UE 2016/679.

**Luca Moroni**
CISA® Certified IT Auditor - ISO/IEC 27001 Certified on Cybersecurity
ITIL Certified on IT Service Management

# Rischio informatico e Assicurazione: la ricerca Via Virtuosa

Il White Paper pubblicato da Via Virtuosa nel 2017 offre un'analisi dello stato dell'arte dell'esposizione al rischio Cyber e della consapevolezza rispetto al tema assicurativo nelle imprese.
Il primo dato che emerge è che il CIO, che nelle PMI si fa carico quotidianamente delle scelte in ambito Sicurezza Informatica, non contempla la possibilità di affidare la tutela del rischio residuo alle Assicurazioni.

**La ricerca**
E' stata presentata una prima indagine sull'esposizione al Rischio Cyber che ha coinvolto un campione di 68 aziende del Nord-Est basata sulla Metodologia ENISA dell'Agenzia Europea per la Sicurezza delle Reti e dell'Informazione. Circa il 30% del campione si posiziona nell'area ad elevata esposizione al rischio, con un impatto significativo sul business in caso di incidente. Chi si trova in questo quadrante viene invitato ad esternalizzare il rischio. La seconda indagine si focalizzava sulla sensibilità dei CIO al tema della Cyber Risk Insurance ed ha coinvolto un campione di 63 aziende del Nord-Est, che hanno risposto a 12 domande definite dal Broker Assicurativo Margas coinvolto nella ricerca. L'obiettivo era comprendere il livello di competenza del CIO sulla materia e lo scenario esistente in azienda. Nel campione, delineato sulla base di tre caratteristiche – fatturato, settore e numero dipendenti – prevale il settore industria e servizi al di sopra di 20 Mln Euro di fatturato e con più di 100 addetti.

**Fattori critici**
Danno reputazionale, fermo d'attività e perdita/non accesso a dati aensibili emergono come fattori critici di cui occuparsi. Il campione, in ottica Cyber Security quasi "virtuoso", attua piani di Business Continuity e Disaster Recovery nel 50-60% e un controllo delle vulnerabilità nel 60% dei casi. Ci si occupa poco invece di formalizzare delle procedure/policy (28%) probabilmente per scarso committment da parte della direzione. Ugualmente basso è il livello di attenzione alla creazione di unità interne o esterne per la gestione di un'eventuale crisi reputazionale (18%).
Il CIO è in grado di affermare che le cause di incidenti IT risiedono in modo equamente ripartito in attacco informatico (soprattutto ransomware), guasto ed errore umano (interno/esterno) ed individua per il board i settori aziendali in cui l'impatto di un fermo d'attività sarebbe più pesante.

**Tema assicurativo**
Il 60% dei CIO non si è mai interessato fin qui del tema assicurativo, ma ha appurato che esistono in azienda un 30% di Polizze Elettroniche (copertura dell'hardware) e un 5% di Polizze Cyber.
Grazie al coinvolgimento di tre CIO abbiamo elaborato 18 domande che tutti vorrebbero fare, prima di affrontare una valutazione di una Cyber Risk Insurance per l'azienda. Il documento si rivolgeva anche alle compagnie assicurative che iniziavano nel 2017 a presentare questi prodotti. Si voleva far comprendere che era ed è necessario premiare l'adozione di una politica di prevenzione, che permetta di misurare un rischio proporzionale alle misure di sicurezza adottate, sulla base di una metodologia di analisi condivisa e riconosciuta come potrebbe essere la norma ISO 27001. Il documento è stato presentato in alcuni convegni nazionali e internazionali ed ha ottenuto il patrocinio di numerose associazioni, fra cui quella nazionale per le imprese assicuratrici, otre ad avere avuto richiami sulla stampa. (1) Il documento è scaricabile gratuitamente al link https://www.viavirtuosa.com/whitepaper/ previa verifica dei requisiti dei destinatari. Nel corso del 2017 era possibile fare una donazione destinata al progetto Generazione Z dedicato alla diffusione della consapevolezza dei rischi tra i cosiddetti Nativi Digitali o Millennials.

(1) Tra i quali: la testata ZEROUNO N.414 - dicembre 2017 Pag. 28-32 "Cyber Insurance: perché coinvolgere il CIO". Corrire Imprese Nord Est gennaio 2017 "Cyber Furti e danni collaterali". Report Clusit 2017 pag.104-112 "Assicurazioni e Cyber Risk/ Sfida assicurativa al CIO detentore della Security Effectiveness aziendale". Nel Web in uno dei più importanti Blog sui temi di Cybersecurity "Security Affairs".





**Marco Soffientini**
Docente Università degli Studi di Roma UnitelmaSapienza; esperto di Privacy e Diritto delle Nuove Tecnologie; Privacy Officer certified in accordo a ISO/IEC 17024:2003; Coordinatore Nazionale Comitato Scientifico Federprivacy; membro dell'Istituto Italiano per la Privacy; membro Comitato di Delibera

# La sicurezza dei dati con il GDPR

Come precisato nelle linee guida interpretative del Regolamento UE 679/2018 prodotte dall'Autorità Garante per la protezione dei dati personali, a partire dal 25 maggio 2018 tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avveniva in precedenza – devono notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85).

**Data Breach**
Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati – valutazione che spetta, ancora una volta, al titolare. Se la probabilità di rischio per gli interessati è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell´art. 34, che coincidono solo in parte con quelle menzionate nell'art. 32-bis del Codice Privacy.

**Sicurezza dei dati**
Come si evince dalla disciplina europea in tema di data breach, la sicurezza dei dati è demandata al titolare, al quale è attribuito il compito di valutare i rischi inerenti al trattamento (vedi Considerando 83), al fine di mantenere la sicurezza e prevenire trattamenti illeciti. La disciplina specifica è contenuta nella Sezione II, articoli 32-34. Un trattamento di dati personali è "sicuro" quando si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche in maniera tale da limitare le minacce alla:

- riservatezza (R)- assicurandosi che le informazioni siano accessibili solo a chi è autorizzato ad averne accesso;
- integrità (I) - assicurandosi che le informazioni siano modificabili solo da chi è autorizzato, quando necessario e che non siano danneggiate o modificate per caso o con dolo;
- disponibilità (D) - assicurandosi che utenti autorizzati abbiano accesso alle informazioni, quando necessario.

Inoltre, quando un tipo di trattamento prevede l'uso di nuove tecnologie che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto ad effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

**Valutazione del rischio e accountability**
In conclusione, la valutazione del rischio è fondamentale per "misurare" il principio dell'accountability o di responsabilizzazione, che consiste nel dovere del titolare del trattamento di mettere in atto misure di sicurezza tecniche e organizzative adeguate, al fine di dimostrare che il trattamento è effettuato conformemente al regolamento. Ciò significa che con il GDPR le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1).

**Maria Lilia La Porta**
Avvocato, Consulente privacy, membro della Commissione Tutela dei consumatori e Privacy dell'Ordine degli Avvocati di Roma

# La nuova figura del DPO

Per comprendere le modifiche apportate dal Reg. UE 2016/679 alle figure privacy, è utile procedere ponendo a confronto, secondo una struttura piramidale, i soggetti privacy considerati dal D.lgs. 196/2003 (Codice privacy) con quelli presenti nel nuovo Reg. UE 2016/679. Partendo dall'apice della piramide, in entrambi i testi normativi si rinviene la figura del Titolare del trattamento.

**Titolare del trattamento**
Ponendo a confronto l'art. 4 lett. f) D.lgs 196/2003 e l'art. 4 n.7 Reg. UE 2016/679, si evince che tale soggetto, che può essere una persona fisica o giuridica, presenta le medesime caratteristiche, in quanto soggetto che determina le modalità e finalità del trattamento, con la differenza che nel Reg. UE 2016/679 non è più preso in considerazione il profilo della sicurezza.

**DPO: una nuova figura, autonoma e indipendente, che garantisce l'osservanza della normativa e facilita il Titolare del trattamento facendo da contatto con l'autorità di controllo nazionale.**

**Responsabile del trattamento**
Scendendo nella struttura piramidale, si ha la figura del Responsabile del trattamento. Si tratta di una figura privacy che ha dato luogo a non pochi confronti interpretativi, in quanto per il vecchio Codice era una figura senza dubbio interna alla struttura aziendale, sia che fosse una persona fisica o giuridica, preposta dal Titolare al trattamento dei dati (art. 4 lett. g) D.lgs 196/2003); mentre il nuovo Regolamento ha introdotto un'importante modifica, considerando il Responsabile del trattamento come figura esterna, in quanto tratta i dati personali per conto del Titolare del trattamento (art. 4 n.8 Reg. UE 2016/679).

**Incaricato del trattamento**
Alla base della piramide troviamo poi una serie di soggetti, persone fisiche, che materialmente entrano in contatto con i dati e sono autorizzate al trattamento da parte del Titolare o del Responsabile del trattamento. Tale figura veniva indicata nel Codice privacy quale Incaricato del trattamento (art. 4 lett. h D.lgs 196/2003), mentre non è espressamente individuata nel Reg. UE 2016/679. Tuttavia, nel testo del Regolamento si rinviene la medesima figura, che viene indicata quale Persona autorizzata.

**Data Protection Officer**
Infine, al lato della piramide, quale soggetto estraneo alla struttura gerarchica piramidale sinora presa in considerazione, è possibile individuare il DPO (Data Protection Officer). Si tratta di una nuova figura, dotata di autonomia ed indipendenza, introdotta dal Reg. UE 2016/679 al fine di garantire l'osservanza della normativa in materia di protezione dei dati, di facilitare le attività del Titolare del trattamento ed essere un punto di contatto con l'autorità di controllo nazionale e le cui caratteristiche e competenze sono indicate negli artt. 37-38-39 del Regolamento medesimo. Infatti il Regolamento non definisce tale soggetto, ma viene individuato sulla base dei requisiti che deve possedere e dei compiti che deve svolgere. In particolare il Regolamento UE 2016/679 all'art. 37 individua alcune specifiche ipotesi di designazione obbligatoria del Data Protection Officer (DPO) o Responsabile della protezione dei dati (RPD). Le ipotesi di obbligatorietà della nomina previste dall'art 37 sono:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Il DPO può essere interno o esterno, deve essere un soggetto dotato di particolari competenze, in particolare deve conoscere la materia della protezione dei dati, deve avere delle conoscenze tecniche/tecnologiche e deve avere dimestichezza con le politiche e le scelte aziendali. Nel caso di DPO interno, deve essere individuato un dipendente dell'azienda, adeguatamente formato, che non sia in conflitto di interessi, ossia che non rivesta ruoli dirigenziali ed al quale vengono affidate dal titolare del trattamento ulteriori mansioni, stabilendo quanto tempo e con quali risorse deve svolgere le funzioni di DPO. In tale caso deve essere predisposto un atto di designazione. Nel caso di DPO esterno, dovrà essere effettuata una valutazione delle proposte ricevute e procedere con la redazione di un contratto di servizi con il DPO che si intende nominare. In entrambi i casi il Titolare del trattamento dovrà procedere con la comunicazione al Garante del DPO nominato.

**Data Protection Officer**