SICUREZZA PRIVATA: NUOVE FIGURE PROFESSIONALI

Data Protection Officer e Security Manager nelle Imprese di Vigilanza Privata

FederSicurezza

Ufficio Studi ed Analisi di settore

COLLANA QUADERNI

Ottobre 2019

Numero 15

SICUREZZA PRIVATA: NUOVE FIGURE PROFESSIONALI

Data Protection Officer e Security Manager nelle Imprese di Vigilanza Privata

A cura del Commissario della Polizia di Stato **Vincenzo Acunzo** - Analista del Dipartimento della Pubblica Sicurezza

Si ringrazia il dott. Mattia Iurato che ha curato la realizzazione del paragrafo relativo al GDPR

Grafica ed impaginazione a cura di Mariarosaria Sardelli

Presentazione del Presidente di FederSicurezza

Avv. Luigi Gabriele

Non sempre è possibile mantenere gli impegni che si assumono, pur impegnando al massimo la propria organizzazione.
Siamo, infatti, in palese ritardo con la produzione di quei Quaderni che, pure, hanno sempre, e sempre ne saremo grati, suscitato interesse, e a volte anche plauso, in quei cortesi lettori che ci seguono.
Speriamo di rimediare, almeno in parte, al non voluto rallentamento, sottoponendo al Vostro esame argomenti di non poco conto ai quali va dedicata la giusta attenzione.

Il momento che il mondo generalmente, e forse troppo genericamente, viene definito "della sicurezza", è in continuo travaglio, peraltro in una "sala parto" forse troppo affollata di medici generici, pochi ginecologi specializzati, non sufficienti ostetriche e...fin troppi anestesisti, non è da tempo dei migliori. Anzi, tutt'altro!

È però, questo mondo variopinto, coincidente con un mercato in costante evoluzione e, per molti aspetti, imprenditorialmente appetibile.

È un mondo scaraventato da un territorio di caccia riservato al libero mercato in modo a dir poco affrettato e non con il giusto, necessitato, accompagnamento.

Ed è anche un mondo di corsari che convivono con qualche Sir Francis Drake, un mondo ancora di naviganti a vista che, però, cominciano a intravedere, sulla linea dell'orizzonte, il profilo di sagome imponenti, novelle corazzate imprenditoriali, pronte ad avviare una profonda mutazione genetica di tale pianeta, disorientato da una superfetazione normativa e sottoposto a movimenti tellurici di sempre più elevato, e di fatto incontrollato, grado della scala Mercalli.

Quindi, per andare al concreto, un mondo che non può rinunciare all'informazione che induce alla formazione.

Eccoci per questo di nuovo qui, con la speranza di essere ancora una volta accolti dal Vostro interesse e, di più, dalla Vostra benevolenza!

Grazie

Luigi Gabriele

INDICE

INTRODUZIONE

Sigmund Freud sosteneva che "*...di fatto l'uomo primordiale stava meglio, poiché ignorava qualsiasi restrizione pulsionale. In compenso la sua sicurezza di godere a lungo di tale felicità era molto esigua. L'uomo civile ha barattato una parte della sua possibilità di felicità per un po' di sicurezza*" [1].

La sicurezza diventa in tal modo una delle necessità fondamentali di ogni comunità, che va oltre quelle elementari e fisiologiche di sfamarsi e di sopravvivere; l'uomo ha nella sua scala di bisogni quelli di *salvezza, sicurezza e protezione*[2], che l'hanno spinto ad unirsi in comunità organizzate al fine di soddisfare tali esigenze, ricorrendo sovente anche a forme di autoprotezione.
In questo contesto, un ruolo di sicuro rilievo è giocato - nonostante si possa affermare che notevole è stato il progresso nel campo della sicurezza nel settore pubblico - dal settore privato.
Il bisogno di sicurezza e protezione, in generale, non è solo un'esigenza avvertita dal singolo cittadino, ma anche dalle aziende, tra cui quelle che operano nel settore della sicurezza privata.
E tra i beni che necessitano di adeguata protezione ci sono, oggi più che mai e sempre di più, le informazioni, in particolare quelle personali.

La necessità di emanare un Regolamento europeo per la tutela dei dati personali è nata dalla continua evoluzione del concetto di protezione degli stessi, dovuta principalmente alla diffusione del progresso tecnologico.
La tecnologia attuale consente alle imprese private e alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle proprie attività. Da qui la necessità di instaurare un quadro giuridico più solido e coerente in materia.
A tal fine, l'Unione Europea ha emanato il GDPR, per esteso *General Data Protection Regulation* che, affiancato ad efficaci misure di attuazione, consentirà lo sviluppo dell'economia digitale nel mercato interno, garantirà la tutela dei dati personali delle persone fisiche e rafforzerà la certezza giuridica ed operativa per i soggetti economici e le autorità pubbliche che operano nel settore.

Cercheremo quindi di capire se l'adempimento al GDPR è solo ed esclusivamente un mero onere di *compliance* oppure se può essere sfruttato come vera e propria opportunità di sviluppo e quindi di creazione di valore per le imprese, analizzando, in maniera sintetica, il percorso normativo che ha portato la Commissione Europea ad emanare questa direttiva e descrivendo le principali novità e differenze con le regolamentazioni precedenti.
Analogamente affronteremo l'annosa questione se la funzione di security nelle moderne aziende sia solo un costo o se invece, garantendo il funzionamento e la difesa dai rischi dei processi produttivi aziendali, assicuri o addirittura implementi la capacità delle stesse di produrre reddito.

---

[1] Cit. Sigmund Freud, "Il disagio della civiltà", 1929.

[2] "Piramide dei bisogni di Maslow": nel 1954 lo psicologo Abraham Maslow propose un modello motivazionale dello sviluppo umano basato su una "gerarchia di bisogni", cioè una serie di "bisogni" disposti gerarchicamente in base alla quale la soddisfazione dei bisogni più elementari è la condizione per fare emergere i bisogni di ordine superiore.

LA TUTELA DEL DATO

1. Dati personali: il percorso normativo

Sono dati personali le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.."[3].
Così il Garante della Privacy definisce i dati personali, tema estremamente dibattuto in questi ultimi anni, soprattutto per quanto riguarda il loro trattamento sul web.
La regolamentazione riguardo questo ambito è molto recente; infatti, prima di una specifica normativa, l'unica tutela era fornita, volta per volta, dalle decisioni della Suprema Corte di Cassazione.
Alla fine del XX secolo, per rispettare gli Accordi di Schengen e per dare attuazione alla direttiva europea 95/46/CE[4] del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, venne emanata la Legge 31 dicembre 1996, n. 675, che entrò in vigore nel maggio 1997.
Col passare del tempo, a tale norma si erano affiancate ulteriori leggi, riguardanti singoli e specifici aspetti del trattamento dei dati. La successiva complessità normativa che si era creata in seguito all'approvazione di diverse disposizioni portò all'emanazione del D.lgs. 30 giugno 2003, n. 196[5], che ha riordinato interamente la materia.
Nel 2011 e 2012 altre disposizioni hanno modificato il codice del 2003, in particolare abolendo alcuni passaggi burocratici ed alcune regole riguardanti le informazioni sensibili fornite spontaneamente mediante il proprio curriculum vitae.
In data 25 gennaio 2012 la Commissione Europea ha approvato la proposta di un regolamento sulla protezione dei dati personali, in sostituzione della Direttiva 95/46/CE.
Il 4 maggio 2016 è stato infine emanato il regolamento dell'Unione Europea n. 2016/679, che è entrato in vigore il 25 maggio 2018, il cosiddetto **GDPR** (***General Data Protection Regulation***).

2. GDPR, questo sconosciuto

Questo nuovo Regolamento è stato definito da molti come uno degli atti più rivoluzionari e incisivi in materia di protezione dei dati personali realizzato negli ultimi vent'anni.
Infatti, ben 28 paesi (Italia inclusa) si sono dovuti adeguare ad una serie di regole univoche, rivolte a tutti coloro che trattano i dati personali dei cittadini europei.
Il nuovo regolamento determina una nuova interpretazione dell'attuale Codice della Privacy, vigente solo in Italia. Si assiste ad un vero e proprio cambio di prospettiva, in quanto ora il protagonista della normativa non è più l'interessato, bensì il **dato personale**.
Molto interessate ai nuovi sviluppi, oltre ai cittadini, dovrebbero essere le imprese, anche se pare che ci sia ancora troppa disinformazione sul tema.

[3] Garante per la protezione dei dati personali, "*Cosa intendiamo per dati personali?*"

[4] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*".

[5] Il Codice per la protezione dei dati personali (comunemente noto anche come Codice della privacy) è una norma della Repubblica Italiana, emanata con il Decreto legislativo 30 giugno 2003, n. 196, in vigore dal 1° gennaio 2004.

3. Dalle rivelazioni di E. Snowden al caso Schrems

Per comprendere meglio le forze che si contendono il campo e le dinamiche in atto, partiamo innanzitutto da fatti di cronaca recente.

I documenti diffusi da Edward Snowden[6] e pubblicati dal *Guardian* e dal *Washington Post* nel giugno 2013, che svelano i dettagli di diversi programmi di sorveglianza di massa del governo statunitense e britannico, fino ad allora tenuti segreti, hanno provocato un vero e proprio terremoto.
La tensione a livello parlamentare e giurisdizionale che questo evento ha scaturito si inserisce a pieno titolo all'interno del conflitto regolatorio transatlantico, apparso in tutta la sua evidenza già a seguito dell'introduzione della direttiva europea in materia di protezione dei dati personali (Direttiva 96/45/CE)[7]. Fino al cd. *Datagate*, infatti, la dinamica di confronto a livello di equilibri interni all'Unione Europea aveva visto protagonista essenzialmente la Commissione europea mentre la Corte di Giustizia, normalmente atta ad occuparsi di conflitti di questo genere, si trovava in una posizione più "defilata".

Ma nel 2008 uno studente austriaco ed attivista in materia di protezione dei dati personali, **Max Schrems**, effettuava l'iscrizione al noto social network **Facebook**, di proprietà e gestione dell'omonima società, Facebook Inc., con sede principale a Palo Alto, California. All'atto dell'iscrizione, Schrems rilevava come, al fine di utilizzare i servizi proposti dalla piattaforma, fosse necessario sottoscrivere un contratto con Facebook Ireland, ovvero una controllata di Facebook Inc., sita in territorio irlandese. Pertanto, veniva a verificarsi di fatto un trasferimento di dati dal territorio di uno Stato membro dell'Unione Europea a quello statunitense.
A questo punto, la Corte di Giustizia irrompe definitivamente sulla scena stabilendo che il trasferimento di dati personali di cittadini europei verso gli Stati Uniti non è lecito, e quindi affermando che il trattamento di questi dati è regolato dal diritto dell'Unione europea e non dal diritto di un altro Stato (in questo caso gli Stati Uniti).

La convinzione dell'opinione pubblica, fino al momento di questa pronuncia, era invece che il trattamento dei dati da parte del motore di ricerca "globale" non fosse soggetto alla direttiva UE sui dati personali, poiché era effettuato su potentissimi calcolatori localizzati negli Stati Uniti. O almeno, questo era quello che si era evinto con la decisione sul caso Google Spain[8].
Con la pronuncia Schrems, invece, la Corte ha affermato che Facebook deve considerarsi stabilita nel territorio europeo poiché opera all'interno dello spazio economico europeo, e quindi soggetta al diritto dell'Unione. La Corte mostra definitivamente il suo ragionamento, ossia revocare l'idea che l'attività sulle reti di telecomunicazione e attraverso Internet sia a-territoriale e non soggetta a sovranità statale[9].

---

[6] Informatico e attivista statunitense, ex tecnico della CIA e fino al 10 giugno 2013 collaboratore della Booz Allen Hamilton (azienda di tecnologia informatica consulente della NSA, la National Security Agency).

[7] Op.cit. nota 2

[8] La Corte di Giustizia dell'Unione europea si è pronunciata, in data 13 maggio 2014, in relazione al caso Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González (causa C-131/12). All'origine della vicenda vi è una richiesta con la quale un cittadino spagnolo aveva cercato di ottenere, prima dal gestore del sito e poi da Google, la rimozione di alcuni dati personali pubblicati su un articolo di giornale ritenuti non più attuali.

[9] L'idea è contestata da W. Heintschel Von Heinegg, "Legal Implications of Territorial Sovereignty in Cyberspace".

Con questa progressiva *escalation*, con l'epilogo rappresentato dal caso Schrems, la Corte si concentra sull'ordinamento con il quale i diritti sopracitati sono destinati a interagire, e cioè quello statunitense, affermando però il prevalere della propria competenza. Il contesto in cui si esprime lo "scontro" tra UE e USA risulta del tutto evidente: la prospettiva di due superpotenze internazionali che si fronteggiano per il controllo di una risorsa essenziale: i dati personali[10].

4. La causa USA v. Microsoft Corporation

Un caso esemplificativo del conflitto descritto, che potrebbe rappresentare un punto di svolta, dipenderà dalle scelte che opererà la **Suprema Corte degli Stati Uniti d'America** nella controversia che vede opposta al **Governo statunitense** la società privata **Microsoft Corporation**.

La vicenda inizia nel dicembre del 2013, quando nell'ambito di un'indagine per traffico internazionale di droga, la *United States District Court for the Southern District of New York* autorizza l'acquisizione dagli USA di informazioni, associate ad account di posta elettronica, archiviate su server di proprietà della Microsoft Corporation, collocati in Irlanda.
Poiché i server si trovavano al di fuori del territorio americano, Microsoft riteneva che per rilasciare le informazioni dovevano prima sussistere le condizioni previste dal *Mutual Legal Assistance Treaty (MLAT)*[11] esistente tra USA e Irlanda.
Il tribunale americano aveva inizialmente ritenuto, invece, che la normativa da prendere in considerazione fosse quella interna statunitense (e non il MLAT), a prescindere dalla localizzazione geografica dei dati, confermando la decisione in più gradi di giudizio.
Fino a quando, la *District Court* del *Second Circuit*, cui la società americana si era ulteriormente appellata e nel cui giudizio erano intervenute sia il Governo irlandese che diverse società operanti nel campo dell'ICT e dell'informazione (tra cui Apple, Amazon, la CNN, The Washington Post ed altre) affermava la necessità di ricorrere alle procedure del Trattato internazionale con l'Irlanda, dando ragione a Microsoft.

La vicenda è tuttora aperta, poiché il Governo statunitense ha deciso di portare la questione davanti alla **Suprema Corte**, e la battaglia a colpi di ricorso ha travalicato i confini degli Stati Uniti attirando l'attenzione di Istituzioni, società ed esperti in *data science* da tutto il mondo, che hanno depositato vari documenti nell'ambito di questo giudizio per fornire volontariamente informazioni secondo il loro punto di vista.

La decisione, in particolare, potrebbe aggiungere un nuovo, significativo capitolo al conflitto USA-UE, trattandosi dell'acquisizione di dati conservati dalla "succursale" Microsoft Ireland, stabilita sul territorio di un Paese membro dell'Unione Europea.

5. La posizione dell'Unione

In questa prospettiva risulta particolarmente interessante esaminare la posizione dell'Unione Europea, espressa nel **documento depositato dalla Commissione UE** nell'ambito del procedimento.

---

[10] "Intorno alla decisione del caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione", V. Zeno-Zencovich.

[11] Un trattato di mutua assistenza giudiziaria (MLAT) è un accordo tra due o più paesi allo scopo di raccogliere e scambiare informazioni nel tentativo di facilitare l'operato giurisprudenziale dei paesi firmatari.

La Commissione europea, come "guardiano dei trattati", ha l'autorità di verificare il rispetto da parte degli Stati membri della normativa dell'Unione Europea, inclusa quella in materia di protezione dei dati personali. Di norma la Commissione agisce solo in caso di questioni strutturali sull'applicazione della normativa dell'UE da parte degli Stati membri, e non in casi individuali, ma data l'importanza del tema ha ritenuto di dover intervenire.

L'Unione Europea, ritenendo che il caso riguardi dati personali conservati in un *data center* gestito da una società "sussidiaria" della Microsoft stabilita nel territorio europeo, attraverso la Commissione, afferma che per la conservazione ed il trasferimento di questi dati verso gli USA si devono applicare le regole UE sulla *Data Protection*. La posizione della Commissione mira ad assicurare un bilanciamento, all'interno di un quadro giuridico che eviti conflitti e favorisca il dialogo, tra protezione dei dati personali e legalità, che sono poi le finalità del GDPR. Ecco perché nel caso in questione verranno applicate proprio le misure previste dal *General Data Protection Regulation*.

Il GDPR, infatti, contiene specifiche previsioni volte ad assicurare che la *data protection* all'interno dell'Unione sia garantita quando i dati personali vengono trasferiti ad un Paese Terzo (Capo V, artt. 44 - 50), e quindi non vi è alcun dubbio che la normativa UE regoli proprio le questioni al centro della controversia in esame.

La Commissione, viene sottolineato nel documento, è perfettamente al corrente che il tema può causare "frizioni" con altri Stati e risultare in violazione del diritto internazionale, ed ha quindi sviluppato un orientamento teso a mitigare questi rischi e ad aiutare la Corte a valutare la controversia.

A tal fine, sottolinea i diritti che il GDPR riconosce alle persone per i dati personali, inclusi i rimedi amministrativi e gli obblighi che devono rispettare i soggetti responsabili del trattamento, ricordando che la prima parola spetta alle autorità di controllo istituite a livello nazionale, che possono comminare sanzioni amministrative, nei casi più gravi, fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente[12].

Dopo aver disciplinato i casi in cui il trasferimento di dati personali all'estero è ammissibile (artt. 45-47), l'art. 48 affronta il "*Trasferimento o comunicazione non autorizzati dal diritto dell'Unione*"[13].
Come risulta chiaro dalla lettura dell'articolo, questa disciplina riguarda il caso di trasferimenti "disposti" da Paesi terzi, ed afferma che essi possono essere effettuati solo in presenza di un Trattato di mutua assistenza giudiziaria (MLAT), che gli Stati Uniti hanno ratificato sia con l'Unione Europea che con l'Irlanda[14].

---

[12] Art. 83, comma 5, del GDPR.

[13] Art. 48: "Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo".

[14] Si veda il Trattato di mutua assistenza legale tra gli Stati Uniti d'America e l'Unione Europea, 25 giugno 2003, 2003 O.J. (L181) 34; ed il Trattato tra gli Stati Uniti d'America e l'Irlanda di mutua assistenza legale in materia criminale, 18 gennaio 2001, S. Treaty Doc. No. 107-9 (2002).

In sintesi, la posizione espressa dalla Commissione Europea sembra potersi riassumere come segue: l'esecuzione dell'ordine del giudice americano nei confronti di Microsoft Corporation, riguardante l'acquisizione di dati conservati da una "sussidiaria" di Microsoft in un *server* localizzato in Irlanda, va valutato nel quadro dei principi riconosciuti dal diritto internazionale, e va considerata la normativa europea sulla protezione dei dati personali, il GDPR, che in caso di trasferimento di dati verso Paesi terzi, giustificato da un interesse riconosciuto, prevede il ricorso alle procedure previste in accordi internazionali, quali il MLAT esistente tra le Parti, sostenendo quindi la posizione di Microsoft.

6. Un altro punto di vista

Tra gli altri documenti versati nel procedimento in qualità di *amici curiae*, risulta particolarmente interessante esaminare il *brief* depositato da ex alti ufficiali della sicurezza nazionale, delle forze di polizia e della comunità *intelligence* degli Stati Uniti, del Regno Unito e della Francia.
Il documento ritiene che il modo migliore per affrontare la controversia non siano le pronunce giurisdizionali (che siano queste riguardanti trattati internazionali o normative statali) ma piuttosto un dibattito legislativo; secondo la posizione espressa nel *brief*, è il **Congresso degli Stati Uniti** e non la Suprema Corte che può bilanciare meglio i diversi interessi che la complessa materia presenta.

L'équipe ritiene che l'eventuale decisione della Corte di affermare l'efficacia extraterritoriale della legge americana darebbe luogo con ogni probabilità all'incremento di inavvertite e non volute conseguenze, a detrimento dell'azione delle forze di polizia e delle agenzie di *intelligence*; ad esempio, l'impulso degli Stati a un progressivo abbandono della cooperazione multilaterale e, quindi, all'unilateralismo.
A sua volta, l'unilateralismo accelererebbe il processo di *data localization* in tutto il mondo, ossia una "localizzazione forzata dei dati" nell'ambito dei confini nazionali.
Quest'ultima eroderebbe la natura aperta di internet, imponendo costi e barriere per l'utilizzo, l'accesso e la conservazione dei dati.
Per di più, i Governi autoritari userebbero ancor di più la *data localization* per controllare ed esercitare il potere sui loro cittadini, limitando il libero scambio di informazioni.
I Paesi "protezionisti", inoltre, la utilizzerebbero per escludere le compagnie straniere dalle loro economie, evidentemente per proteggere le industrie locali, ma a scapito degli altri partecipanti al mercato e del potere di acquisto dei propri cittadini.

Tendenze particolarmente preoccupanti, ad avviso degli *amici curiae*, in un'epoca caratterizzata da un esponenziale incremento del crimine transnazionale e delle diverse forme di minaccia cibernetica.

Altra rilevante problematica potrebbe scaturire dalla competizione delle varie leggi nazionali, tramutandosi in poca chiarezza per le aziende, che sarebbero "*forzate a scegliere tra le leggi di una Nazione che prevede la ricerca e l'accesso ai dati e le leggi di un'altra Nazione che proibisce questi accessi*"[15].

Ne discende, quindi, che la decisione in merito a questa causa potrebbe rendere molto più difficoltoso per le forze dell'ordine e per l'*intelligence* la conduzione di indagini transnazionali. Questo risulta particolarmente vero poiché la normativa di riferimento

[15] Jennifer Daskal, Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issue

appare essere divenuta obsoleta alla luce dell'evoluzione tecnologica, dell'universale adozione della corrispondenza elettronica e dei telefoni portatili e per l'utilizzo del *cloud computing*.

Lo *Stored Communications Act* (S.C.A)[16], infatti, fu emanato dal Congresso nel 1986 con l'intento di proteggere il diritto alla privacy dei cittadini statunitensi nell'uso di comunicazioni da remoto e servizi computerizzati negli Stati Uniti.
Il Congresso ha quindi riformato la normativa emanando, il 25 maggio 2018, il "*CLOUD Act*".

7. Il "*CLOUD Act*"

La discussione che si è sviluppata intorno al caso USA vs Microsoft Corporation ha innalzato il livello di attenzione dedicato ai sopraesposti temi sull'altra sponda dell'Atlantico, portando alla presentazione presso il Senato degli Stati Uniti, il 6 febbraio 2018, del ''*Clarifying Lawful Overseas Use of Data Act*'' ovvero "*CLOUD Act*"[17].
La proposta, che ha ricevuto l'approvazione ed il sostegno di giganti del web come Microsoft, Google, Apple e Facebook, intendeva apportare modifiche alla legislazione americana, in particolare allo "*Stored Communication Act*".
Le principali linee di intervento, che riguardavano il contrasto di *serious crimes* e del terrorismo, si possono così riassumere:

- ✓ accordi bilaterali: la proposta incoraggia il Governo USA a stipulare accordi con altri Paesi per definire chiari standard per richieste investigative relative a prove contenute su supporti digitali, identificando una serie di presupposti che questi strumenti devono soddisfare; ad esempio, richiede a entrambi i Governi di "certificare" che le leggi e le prassi dell'altro Paese soddisfino gli standard relativi ad un'adeguata protezione dei diritti umani e della privacy. Queste intese devono prevedere, inoltre, periodiche revisioni per assicurare il rispetto delle regole previste in questi ambiti;

- ✓ extraterritorialità dei mandati USA con rispetto dei principi accolti dalla Comunità Internazionale: il CLOUD Act modifica la legislazione americana per rendere chiaro che i mandati americani, rivolti all'acquisizione di dati detenuti da compagnie ICT, possono legittimamente raggiungere i dati conservati ovunque nel mondo. Ma l'efficacia di questi mandati può essere limitata in base ai principi accolti dalla Comunità Internazionale. La proposta attribuisce infatti alle società coinvolte, per la prima volta, un diritto di verifica; una richiesta di sospensione del mandato può essere inviata ogni qual volta vi sia il rischio che questo possa violare le leggi del Paese di stoccaggio dei dati aderente all'accordo;

- ✓ trasparenza: quando un provider ICT riceve una richiesta dalle forze dell'ordine americane, riguardante un cittadino o un soggetto residente nel Paese che ha sottoscritto l'accordo bilaterale con gli Stati Uniti, la società notificherà a quel Governo l'esistenza della richiesta. Ciò consentirà a quel Paese di verificare se i requisiti previsti nell'accordo bilaterale vengono osservati, e gli permetterà di intervenire a livello diplomatico laddove ritenga che la richiesta non sia appropriata.

---

[16] Stored communication Act, 18 U.S.C.
[17] Proposta di legge presentata al Senato americano dai senatori O. Hatch, L. Graham (repubblicani), S. Whitehouse e C. Coons (democratici).

Il 25 maggio 2018 la proposta è diventata legge.
In proposito, occorre rilevare che la legge statunitense è percepita da molti industriali e attori politici come un'interferenza inaccettabile, perché di fatto legalizza lo spionaggio industriale. Secondo le autorità di intelligence francesi, ad esempio, sarebbe in gioco la sicurezza dei dati delle amministrazioni francesi, attualmente archiviate su circa 50.000 server, distribuiti in 120 centri dati.

Il Cloud Act costringe i fornitori di servizi statunitensi e gli operatori digitali a divulgare le informazioni personali dei loro utenti alle autorità, anche se questi dati sono conservati al di fuori degli Stati Uniti. In altre parole, i GAFAM, questi giganti della Silicon Valley, non saranno più in grado di garantire la riservatezza dei loro dati, anche se questi fossero archiviati in Europa.

Il rischio è quindi che il GDPR possa frantumarsi ancor prima di essere efficace. L'arrivo del Cloud Act può infatti rappresentare una minaccia alla segretezza delle attività di qualsiasi azienda europea.

8. La localizzazione forzata dei *cloud services*

Facciamo a questo punto un passo indietro. Una tendenza che si sta sempre più delineando a livello globale, e che potrebbe essere una risposta possibile ai conflitti in atto, è quella che alcuni ordinamenti giuridici stanno adottando.
In termini semplici, consiste in misure che tendono a favorire la conservazione dei dati personali dei propri cittadini all'interno del proprio territorio, costringendo in alcuni casi le compagnie che detengono tali dati a stoccarli in *server* posti nel territorio di quello Stato.

Ciò ha enormi effetti sulle scelte logistico-organizzative e di investimento economico degli operatori privati del settore, che giungono fino a forme di *partnership* "forzate" con società straniere, indicate dai Governi. Dopo le già citate rivelazioni di E. Snowden sono stati ridotti i trasferimenti di dati addirittura all'interno di aree di libero scambio quali l'Unione Europea.

Un esempio evidente di iniziativa che potrebbe condurre ad un profondo cambiamento dell'attuale concetto di *cloud computing* è stata discussa in Europa e riguarda lo sviluppo di una possibile "*virtual Schengen area*".
Si tratta di un tentativo di creare una zona di libero movimento online per i dati, che potrebbe operare accanto all'area fisica di "Schengen", all'interno della quale i controlli ai confini interni sono stati rimossi per facilitare il libero movimento di persone, beni e servizi tra la maggiore parte dei Paesi UE ed EFTA[18].

9. La tendenza globale alla data localization

Come si accennava, iniziative di singoli Stati membri della UE a livello nazionale sono andate addirittura oltre.
La Germania, ad esempio, ha iniziato a voltare le spalle alle compagnie americane, come Verizon, e attraverso aziende di Stato, come Deutsche Telekom - DT, ha iniziato a

[18] La versione digitale di questo modello è stata espressa per la prima volta nel febbraio 2011 durante la discussione sul cyber crime al joint meeting dell'Eu's Law Enforcement and Customs Cooperation Working Parties.

stoccare i dati attraverso i propri *server* domestici.
La DT ha annunciato nell'ottobre 2013 di aver pianificato di costruire una "internetz" esclusivamente tedesca, per mantenere il traffico internet tedesco all'interno dei confini fisici della Germania[19].
Nel febbraio del 2014, la Cancelliera Angela Merkel ha proposto di dar vita a una infrastruttura internet europea per tenere i dati all'interno dell'Europa.
Successivamente la Germania ha annunciato un piano per costituire un'infrastruttura *cloud* tedesca per l'Amministrazione federale (il "Bundes-Cloud")[20].
A seguito di questi annunci compagnie come *Microsoft* hanno scelto di localizzare i propri *data center* per cittadini tedeschi in Germania. In particolare, nel 2015 è stato raggiunto un accordo tra la stessa Microsoft e DT secondo il quale la stessa compagnia telefonica tedesca diviene la "*data trustee*" per gli utilizzatori in Germania dei servizi Microsoft.

In Francia il Governo ha preso iniziative per favorire la costituzione di *data center* locali, riferendosi ad essi come *"le cloud souverain"*, nell'intento di limitare i *cloud services* a compagnie francesi che operano in Francia. Sono stati investiti, infatti, 150 milioni di euro in due compagnie francesi – Numergy e Cloud Watt – per costruire una infrastruttura *cloud* domestica.

A livello globale, come detto, numerosi Stati hanno introdotto legislazioni sulla *Data Localization* (Canada, Brasile, India, Australia, Indonesia, Vietnam, Iran, Turchia, Corea, per citarne alcuni).

La Cina ha adottato una legge sulla localizzazione forzata dei dati nel giugno 2017, la *Cyber security Law,* che chiede agli operatori di "*critical information infrastructure*" di conservare i dati di *business* e le informazioni personali dei cittadini cinesi, in Cina. La nuova legge prevede che tutti i dati online di chi vive e lavora in Cina siano gestiti da *server* cinesi, per evitare minacce da *hacker* e limitare il cyberterrorismo. Per effetto di queste misure Amazon è stata costretta a vendere a *Beijing Sinnet Technology,* azienda cinese di cui era già partner, gli asset relativi ai servizi *cloud* per circa 300 milioni di euro.
Infine, seguendo il *trend* di altre compagnie, che alla fine dell'anno scorso hanno iniziato a riallocare i propri *data center* per osservare i requisiti della localizzazione dei dati in Cina, Apple ha annunciato che aprirà un *data center* in Cina in osservanza di quanto richiesto dalla legge[21].

---

[19] Frank Dohmen e Gerald Traufetter, "Spy-Proofing: Deutsche Telekom Pushes for All German Internet", Spiegel Online International, 12 November 2013.

[20] Data Localization Requirements Through the Backdoor? Germany's "Federal Cloud", and New Criteria for the Use of Cloud Services by the German Fed. Admin.

[21] Paul Mozur et al., Apple Opening Data Center in China to Comply with Cybersecurity Law, N.Y. TIMES.

IL DATA PROTECTION OFFICER

1. La necessità di cambiare

Dopo un iter legislativo durato quattro lunghi anni, alla fine è arrivato il nuovo Regolamento dell'Unione Europea n. 2016/679 sulla protezione dei dati, che, come già accennato in precedenza, prende il posto del Codice della privacy, che a sua volta si basava sulla Direttiva n. 95/46/CE.

Questa direttiva, emanata nel 1995, era pensata per regolamentare un'epoca in cui la maggioranza delle persone si scambiava ancora la corrispondenza con fax e francobolli e la gente leggeva le ultime news la mattina sul giornale. Con il mercato digitale e *l'internet of things*, gli scenari sono molto diversi da allora e una riforma generale della normativa sulla protezione dei dati personali era indispensabile per regolamentare i flussi di *big data* che attraversano il pianeta da un estremo all'altro. Per questo era fondamentale il conseguimento di un unico ombrello normativo all'interno dell'UE[22].

Sono destinati a diminuire gli adempimenti formali, come la notificazione dei trattamenti al Garante, anche se la tenuta di registri di trattamento sembra confermare un certo profilo burocratico, ma solo a livello residuale, poiché sono privilegiati aspetti di tutela sostanziale.
Rientrano in questo discorso la valutazione dei rischi, il principio dell'*accountability*, la valutazione dell'impatto dei trattamenti sulla protezione dei dati e la eventuale verifica delle prescrizioni da adottare presso le autorità di controllo.
Alcuni istituti, inoltre, vengono estesi nella loro applicazione: ad esempio la notificazione dei dati e il diritto all'oblio. Sulla figura del *Data Protection Officer* vengono poi riposte molte aspettative, in quanto ritenuto il ruolo chiave per "l'efficientamento organizzativo partendo dalla corretta gestione delle informazioni"[23].

2. Le novità per le imprese

Sono molte, oltre che "invasive", le novità previste dal GDPR per le imprese, che dovranno rivoluzionare profondamente i propri processi e le proprie "abitudini" riguardo il trattamento dei dati personali.

Ad esempio, il nuovo regolamento UE in materia di privacy introduce condizioni di parità tra le imprese dell'UE e le imprese di paesi extra UE che forniscono beni e servizi ai cittadini europei, poiché tutte, d'ora in avanti, devono rispettare le stesse norme in materia di protezione dei dati.

Le principali novità per le imprese sono: l'obbligo di tenere un registro dei trattamenti, l'*accountability*, il *data breach*, la *privacy by design and by default*, il *data protection impact assessment* e il nuovo sistema di sanzioni e responsabilità.
Lo strumento base introdotto dal Regolamento in tema di *compliance* è il registro dei

[22] Le tematiche affrontate di qui in avanti sono ben esposte nella "Guida alle novità", "Privacy e regolamento europeo 2016/679".

[23] "il dado è tratto" di Lorenzo Notari.

trattamenti, ex art. 30, rivolto a tutti i titolari e responsabili del trattamento, eccetto gli organismi con meno di 250 dipendenti, ma solo se non effettuano trattamenti a rischio.
Il registro costituisce uno strumento fondamentale per consentire al titolare e al responsabile di effettuare la valutazione e l'analisi del rischio, oltre che per offrire al Garante un quadro completo all'atto della verifica della conformità al Regolamento.
L'obbligo di tenere un registro delle attività di trattamento è una premessa indispensabile per poter dimostrare la conformità ai principi di protezione dati. Si tratta, prima ancora di un adempimento giuridico, di un vero e proprio adempimento logico ed operativo, in quanto utile e strumentale ai soggetti attivi del trattamento.
Il contenuto del registro deve ricomprendere: finalità del trattamento, categorie di interessati e di dati personali trattati, categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi o organizzazioni internazionali, descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32.1.

L'adozione di un registro dei trattamenti, da un lato, impone ai soggetti attivi del trattamento di censire le banche dati e i trattamenti posti in essere, in modo da avere un utilissimo strumento operativo; dall'altro, serve per conservare in maniera ordinata, facilmente ricostruibile a posteriori e verificabile da terzi, l'adozione delle misure adeguate ed efficaci volte ad attuare il principio di responsabilizzazione.

Nella nostra lingua manca un esatto termine equivalente, in quanto "**accountability**" accomuna profili presenti in concetti differenti, quali quello di responsabilizzazione ma anche di rendicontazione.

Il GDPR definisce, all'art. 5.2, il principio di responsabilizzazione nel senso che il titolare del trattamento è competente per il rispetto di tutti i principi di legittimità ed è in grado di comprovarlo. All'art.5, infatti, il GDPR individua nel titolare il soggetto competente a garantire il rispetto dei principi posti dalla nuova disciplina (liceità, correttezza, esattezza ecc.) e stabilisce poi che, oltre a dover garantire il rispetto dei suddetti principi, questo deve essere in grado di "comprovarlo", rendendo quindi il titolare del trattamento "accountable", ossia "responsabilizzato".

Il concetto di "accountability" è ulteriormente delineato dall'art. 24 del Regolamento, che prevede che il Titolare del trattamento debba mettere in atto (nonché riesaminare ed aggiornare) adeguate misure tecniche ed organizzative, per garantire ed essere in grado di dimostrare che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina. Le misure da adottare vanno valutate di volta in volta, tenendo in considerazione una serie di elementi tra cui la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche[24].

In sostanza, la nuova normativa sposta l'onere della prova sul titolare del trattamento, lasciandogli maggiore discrezionalità abolendo le "misure minime" di sicurezza presenti nel Codice della privacy.
L'obiettivo di tale riforma è quello quindi di rendere "acccountable" il titolare del trattamento, poiché egli non è più mero esecutore di un elenco di misure imposte da una norma, ma diviene responsabile delle misure operative e tecniche che riterrà opportune, efficaci e dunque adeguate a salvaguardare i dati che tratta.

Per "**Data Breach**" si intende un incidente di sicurezza in cui dati sensibili protetti o riservati

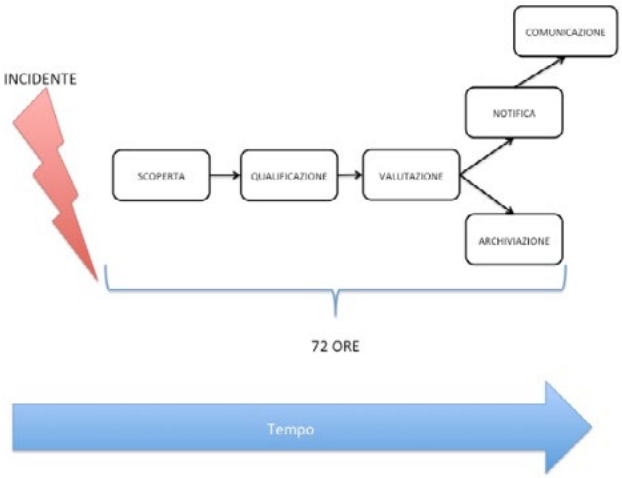
[24] "L'accountability nel Regolamento Generale sulla protezione dei dati", a cura di Andrea Reghelin.

vengono consultati, copiati, trasmessi, utilizzati o rubati da un soggetto non autorizzato.
Solitamente il *data breach* si realizza con una divulgazione di dati riservati o confidenziali in maniera volontaria o involontaria.
Si possono distinguere tre tipi di violazioni:

- ✓ violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- ✓ violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- ✓ violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali[25].

Con l'art. 33 il GDPR impone al titolare del trattamento di notificare all'autorità di controllo la violazione entro 72 ore dal momento in cui ne viene a conoscenza. Quando, però, il titolare può essere ritenuto "cosciente" della violazione?
Nelle linee guida, il Gruppo WP 29[26] ritiene che debba considerarsi "a conoscenza" il titolare che abbia un ragionevole grado di certezza in merito alla verificazione di un incidente di sicurezza.

Individuato il *data breach*, dal 25 maggio 2018 l'obbligo di notifica è esteso a tutti i titolari di trattamento, qualora la violazione rappresenti un rischio per i diritti e le libertà dell'interessato; laddove invece questi rischi fossero ancora più elevati, il titolare dovrà avvertire l'interessato senza indebito ritardo (art. 34). La direttiva 95/46/CE prevedeva invece l'obbligo di notifica solo per i fornitori di servizi di comunicazioni elettroniche accessibili al pubblico e per particolari categorie di trattamenti (dati biometrici, dossier sanitario e pubbliche amministrazioni).
Con l'esponenziale crescita dei *data breach,* quindi, il legislatore europeo ha ritenuto necessario estendere l'obbligo di notifica a tutti i titolari.



[25] "GDPR e data breach, ecco le linee guida per l'applicazione" di Alessandro Frillici - Avvocato, Patrocinante in Cassazione, Foro di Milano e Patrizia Ghini - Dottore commercialista, Consulente direzionale.

[26] Il Gruppo di lavoro WP29 (working party article 29) è stato istituito dall'art. 29 della direttiva 95/46; di tratta è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta.

Un'altra grande novità introdotta dal nuovo regolamento è la cd. "**privacy by design**", un intervento proattivo per le aziende che dovranno sviluppare modalità operative, configurazioni e misure di sicurezza in grado di salvaguardare la riservatezza, l'integrità e la disponibilità dei dati personali. Il titolare del trattamento dovrà, infatti, attuare fin da subito le adeguate misure tecniche ed organizzative per integrare le garanzie necessarie al fine di soddisfare i requisiti del regolamento e tutelare i diritti delle persone interessate.

I principi alla base del sistema sono:

- ✓ prevenire, non correggere, cioè i problemi vanno valutati nella fase di progettazione;
- ✓ privacy incorporata nel progetto;
- ✓ massima funzionalità, in maniera da rispettare tutte le esigenze;
- ✓ sicurezza durante tutto il ciclo del prodotto o servizio;
- ✓ trasparenza;
- ✓ centralità dell'utente[27].

Per "**privacy by default**" si intende, invece, che la tutela della protezione del dato deve diventare l'impostazione predefinita per l'organizzazione**.** Inoltre, specifica la direttiva all'art. 25, sempre per impostazione predefinita, non deve consentirsi l'accesso di dati personali a un numero indefinito di persone fisiche senza l'intervento dell'interessato; e aggiunge che il principio della protezione dei dati *di default* deve essere preso in considerazione anche nell'ambito degli appalti pubblici[28].
Il legislatore impone quindi alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito (by default), gli strumenti (by design) a tutela dei dati personali**.**

L'intento di porre al centro dell'interesse della direttiva l'utente finale e i suoi interessi e diritti si riscontra anche con l'introduzione del "**Data Protection Impact Assessment**", ossia la valutazione d'impatto sulla protezione dei dati.
Tale istituto mira a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità e gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche, effettuando una valutazione del livello del rischio e determinando come mitigarlo.

L'art. 35 chiarisce che la valutazione di impatto è obbligatoria quando il trattamento "presenti un rischio elevato per i diritti e le libertà delle persone fisiche"**.**
Quando si fa riferimento al concetto di rischio nel contesto giuridico della protezione dei dati, e si fa riferimento ai "diritti e le libertà" degli interessati, si pensa subito al diritto alla privacy, ma questo può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

Lo stesso articolo, al comma 3, fornisce inoltre alcuni esempi di casi nei quali un trattamento "possa presentare rischi elevati":

- ✓ una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significa-

[27] "Privacy by design e by default", a cura del sito protezionedatipersonali.it.

[28] "Guida alle novità", "Privacy e regolamento europeo 2016/679", op. cit. alla nota 19.

tivamente su dette persone fisiche;
- ✓ il trattamento, su larga scala, di categorie particolari di dati personali, o di dati relativi a condanne penali e a reati;
- ✓ la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Riprendendo l'art. 35 del GDPR, il 4 aprile 2017 il WP 29 ha fornito delle linee guida in materia per cercare di chiarire come e quando effettuare una DPIA. Il Gruppo di lavoro si è soffermato principalmente su quando considerare un trattamento "rischioso", individuando 9 criteri[29].
Il DPIA va inquadrato come uno strumento essenziale e fondamentale per tutti i titolari e responsabili del trattamento per il nuovo approccio alla protezione dei dati personali voluto dal legislatore comunitario e fortemente basato sul principio della responsabilizzazione (cd. *accountability principle)*[30].

Il legislatore europeo con questa riforma ha voluto rendere il quadro regolatorio ben più severo, stabilendo *ex ante*, a differenza di quanto avveniva in precedenza, alcuni criteri per la ponderazione delle sanzioni amministrative pecuniarie; i quali vengono elencati all'art. 83 paragrafo 2. Nello specifico ne vengono analizzati alcuni:

- ✓ la natura, gravità e durata della violazione;
- ✓ il carattere doloso o colposo della violazione;
- ✓ il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi.

Con riferimento al primo criterio, sarà compito dell'autorità nazionale competente deci-

---

[29] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679. Di seguito i 9 criteri:

- valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" ;
- processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche";
- monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico";
- dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali, nonché dati personali relativi a condanne penali o reati;
- trattamento di dati su larga scala;
- creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
- dati relativi a interessati vulnerabili (es. minori, dipendenti nonché i segmenti più vulnerabili della popolazione che richiedono una protezione speciale);
- uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc;
- quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto."

[30] "Il Data Protection Impact Assessment "DPIA": cos'è e come svolgerlo", a cura dell'Avv. Andrea d'Agostino Senior Legal & Data Protection Counsel Gruppo Mondadori e Dott.ssa Gioia Girotto.

dere la misura più o meno severa del risarcimento. Il legislatore europeo, all'interno del regolamento, dimostra la tendenza ad incoraggiare l'utilizzo delle sanzioni pecuniarie con un approccio "ponderato" ed "equilibrato". L'obiettivo ultimo rimane, infatti, quello di incentivare le società al rispetto della *privacy by design e privacy by default*.

Il secondo criterio, invece, entra nel merito del dolo o della colpa. Sarà compito della giurisprudenza emergente stabilire con più chiarezza i limiti da non oltrepassare.

Con il terzo, viene sottolineata l'importanza di una solida cooperazione con l'autorità di controllo atta a preservare i diritti degli interessati.
Stabiliti i criteri, il regolamento, negli articoli seguenti, disciplina le ipotesi per cui è prevista la pena pecuniaria; dividendole in due gruppi.

Per il primo gruppo è prevista una pena che può raggiungere i 10 milioni di euro o, se superiore, il 2% del fatturato mondiale.
Di seguito alcuni esempi delle violazioni contenute nel primo gruppo:

- ✓ violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- ✓ trattamento illecito di dati personali che non richiede l'identificazione dell'interessato;
- ✓ mancata o errata notificazione e/o comunicazione di un *data breach* all'autorità nazionale competente;
- ✓ violazione dell'obbligo di nomina del DPO;
- ✓ mancata applicazione di misure di sicurezza.

Per il secondo gruppo, invece, gli importi vengono raddoppiati (20 milioni ed eventualmente il 4% del fatturato mondiale), e le circostanze più comuni sono:

- ✓ inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'autorità nazionale competente;
- ✓ trasferimento illecito *cross-border* di dati personali ad un destinatario in un Paese terzo[31].

L' apparato sanzionatorio risulta essere più severo poiché il regolamento, tramite strumenti come i sistemi proattivi di mitigazione del rischio, la rendicontazione e la valutazione di impatto, concede la possibilità alle aziende di avviare sin da subito le dovute valutazioni per conformarsi al nuovo regolamento senza violazioni di alcun tipo riguardo il trattamento dei dati.

3. La necessità di una nuova figura: il DPO

Per uniformarsi al GDPR, quindi, non basteranno adempimenti formali alle nuove disposizioni, ma sarà necessario un nuovo approccio per le organizzazioni.

Tra gli adempimenti di più ampio impatto sul mercato vi è certamente la designazione del **responsabile della protezione dei dati personali**, ovvero del ***Data Protection Of-***

[31] GDPR: le sanzioni. Gruppo di lavoro articolo 29, linee guida provvisorie. A cura della redazione di Altalex.

ficer (DPO), figura già presente nelle organizzazioni più complesse anche nel mercato italiano, ma che è ora obbligatoria per tutta la pubblica amministrazione e in alcuni casi anche in ambito privato.

Il responsabile della protezione dei dati, infatti,è oggi obbligatorio solo quando il trattamento è svolto da un'autorità o da un organismo pubblico (salvo che per le attività giudiziarie) o, in ambito privato, quando le attività principali del titolare o del responsabile consistono in operazioni che, sotto ogni profilo, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala (rientrano per esempio in tale categoria gli operatori di telecomunicazione, gli operatori che effettuano profilazione per finalità di marketing comportamentale oppure per erogare premi assicurativi, localizzazione tramite app, ecc.).

Il DPO in ambito privato è obbligatorio anche per tutte le organizzazioni che utilizzano come attività principale dati sensibili (o meglio particolari secondo il regolamento) oppure dati giudiziari su larga scala; rientrano in tale previsione ospedali, assicurazioni e istituti di credito, ecc., o aziende che in generale hanno più di 250 dipendenti.

il GDPR e i garanti europei non definiscono esattamente i requisiti che deve avere questa nuova figura, sottolineando come "le disposizioni non prevedono un albo dei Responsabili della protezione dei dati, che attesti i requisiti e le caratteristiche di conoscenza, abilità e competenza, previste dal citato quadro normativo né richiedono che tali requisiti siano attestati attraverso specifiche certificazioni"[32].
Come negli altri ambiti delle cosiddette "professioni non regolamentate", infatti, si vanno diffondendo schemi di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori.
Tali certificazioni però, rilasciate anche all'esito della partecipazione ad attività formative e alla verifica dell'apprendimento, se possono rappresentare, al pari di altri titoli, uno strumento per valutare il possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, ad una "abilitazione" allo svolgimento del ruolo di DPO.
Tanto è vero che nella sopracitata nota il Garante sottolinea che la capacità di assolvere ai propri compiti da parte del DPO deve essere considerata sia in relazione alle qualità personali e alle conoscenze dello stesso, sia in relazione alla posizione del DPO all'interno dell'azienda o dell'organismo.

Le principali caratteristiche che il responsabile della protezione dei dati deve avere sono:

- ✓ conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del GPDR;
- ✓ familiarità con le operazioni di trattamento svolte;
- ✓ familiarità con tecnologie informatiche e misure di sicurezza dei dati;
- ✓ conoscenza dello specifico settore di attività e dell'organizzazione del titolare/del responsabile;
- ✓ capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/del responsabile.

I complessi compiti affidati al DPO sono previsti solo a livello minimale dal regolamento; sarà quindi discrezione del titolare o del responsabile valutare quale mansioni affidare al DPO.

[32] Dalla Newsletter del 15.09.17 – Nota del Garante ad una azienda ospedaliera.

In generale, il DPO dovrà **informare** il titolare o il responsabile del trattamento, nonché i dipendenti, **in merito agli obblighi derivanti dal regolamento** e fornire, se richiesto, un **parere** in merito alla valutazione d'impatto sulla protezione dei dati e **sorvegliarne** lo svolgimento (DPIA).

Un'altra importante funzione assegnata al responsabile della protezione dei dati personali è quella di **cooperare con l'autorità di controllo** (autorità garante della privacy), fungendo da punto di contatto tra questa e l'organizzazione.

Infine, dovrà **monitorare il rispetto della *compliance*** con il Regolamento, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale, e controllare che le violazioni dei dati personali siano documentate, notificate e comunicate (c.d. *data breach notification management*).

Nell'eseguire i propri compiti, il responsabile della protezione dei dati dovrà considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il candidato DPO ideale in molti casi potrebbe occupare una posizione dirigenziale o manageriale, fermo restando l'obbligo di riferire al vertice gerarchico; un profilo *senior* potrà garantire maggiore indipendenza rispetto ad uno *junior*, soprattutto per assicurare in modo effettivo la non ingerenza nelle proprie attività da parte del titolare.
Inoltre, potrà essere interno e quindi nominato tra i dipendenti dell'organizzazione, oppure esterno e quindi essere svolto da una società o un pool di professionisti; in ogni caso, tutti i soggetti coinvolti devono possedere i requisiti previsti dalla normativa.

4. Le novità per i cittadini

Sebbene all'art. 1 dei "considerando" venga specificato come l'interesse principe della nuova direttiva sia "la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale", si registra uno squilibrio tra le informazioni trasmesse al cittadino, al fine di renderlo pienamente conscio del proprio ruolo, rispetto al sovraccarico di informazioni che vengono veicolate verso le aziende.

Spesso, infatti, gli unici tentativi di informare i cittadini riguardo le novità contenute nel GDPR sono messaggi lunghi e tecnici che appaiono sotto forma di *pop-up* o finestre internet da chiudere per poter continuare ad usufruire del servizio.

Eppure, nonostante la poca consapevolezza, sono tante le novità per il cittadino, o meglio "l'interessato", che passa da essere mero spettatore dell'utilizzo e abuso di utilizzo dei propri dati, a parte attiva del rapporto, vedendosi riconoscere nuovi e più pregnanti diritti.

Il capo III della normativa, infatti, è dedicato ai "**diritti dell'interessato**". Questa sezione del GDPR si prefigge l'obiettivo di delineare rapporti interni, diritti e possibilità in capo al cittadino, in modo che il rapporto con il titolare o responsabile non si esaurisca con la comunicazione dei dati ma perduri per tutto il rapporto.

Il primo vero diritto per il cittadino è quello di rifiutare di diventare una persona "interessata", rifiutando quindi il trattamento dei propri dati. Ovviamente però questa possibilità non sempre è effettiva in quanto in molti rapporti fornire i propri dati è obbligatorio e vincolante.
Una volta diventato "interessato" però, poiché quei dati rappresentano il cittadino e continuano a rappresentarlo anche durante e dopo il trattamento, egli ha il diritto di monitorare in tutto e per tutto e in qualunque momento cosa avviene ai propri dati: per cosa sono utilizzati, modificarli e persino revocare il consenso per una certa organizzazione[33].

In questo senso si inserisce il diritto di accesso ai dati che rimarca il rapporto indissolubile tra utente e dati personali, per cui la persona interessata ha sempre il diritto di ottenere dal titolare, senza alcun aggravio economico, la conferma che vi sia in corso un trattamento dei propri dati e, in caso positivo, accedere alle informazioni inerenti.
Il diritto di accesso rappresenta, proprio per il potere che conferisce all'utente, una porta aperta sull'operato del titolare del trattamento riconoscendo, ad ogni cittadino, di controllare nel tempo le tracce lasciate dai propri dati e di intervenire, eventualmente, per cambiare le cose, ad esempio rettificandoli qualora questi fossero inesatti (diritto di rettifica).

Il diritto all'oblio può essere definito come il diritto di un individuo ad essere dimenticato, o più precisamente, a non essere più ricordato per fatti che lo riguardano e che in passato sono stati oggetto di cronaca.
Dopo la famosa decisione della Corte di Giustizia europea "Google Spain" del 2014[34], si parla di diritto all'oblio soprattutto riguardo i motori di ricerca e in generale la libertà di stampa e di manifestazione del pensiero; ogni motore di ricerca, infatti, è tenuto a valutare ogni richiesta fatta da una persona fisica di cancellare i link che rendano accessibili le fonti di una notizia che la riguarda nel caso in cui ritenga che questa sia inesatta, non vera e lesiva della sua immagine, o quando ritenga che per il tempo passato, o altre situazioni, legate al bilanciamento tra la tutela della persona e il diritto di informazione dei cittadini, la conoscenza della notizia non sia più di interesse pubblico.

L'art. 17 del GDPR, però, nonostante la rubrica "diritto alla cancellazione" ("diritto all'oblio") possa trarre in inganno, incide pochissimo su questa problematica.

La norma, infatti, introduce alcune precisazioni riguardo le nuove tutele contenute nel regolamento:

- ✓ il diritto di opposizione dell'interessato, a condizione che non sussista alcun interesse legittimo prevalente del titolare o che i dati siano trattati per finalità di marketing diretto;
- ✓ il diritto alla cancellazione dei dati "sensibili" in casi esplicitamente previsti da leggi nazionali;
- ✓ la cancellazione obbligatoria quando i dati raccolti riguardino minori di 16 anni (o dell'età che ciascun Stato potrà fissare purché non inferiore a 13 anni) senza il consenso di chi ha la responsabilità genitoriale.

Ma la vera novità riguarda il paragrafo 2 dell'articolo, in cui viene inserito il dovere specifico per il titolare che riceva una richiesta di cancellazione, non solo a suo carico ma di

[33] "Diritti individuali nel GDPR", EU GDPR Compliant.

[34] Op. cit., si veda in merito la nota 7.

"qualsiasi immagine, copia o riproduzione dei suoi dati personali", quando i dati che ne sono oggetto siano stati "**resi pubblici"** dal titolare stesso.
Per ottemperare alla richiesta di cancellazione di qualunque copia o riproduzione dei dati da parte dell'interessato, il titolare non solo dovrà essere a conoscenza di chi siano gli altri titolari che sono entrati in possesso dei dati in questione, ma dovrà anche segnalare loro il possibile illecito (lasciando alla responsabilità di questi di valutare se essa debba o no essere accolta anche da loro).
In sostanza, si aggiunge il dovere del titolare, che abbia reso pubblici i dati, di diventare un "**tramite obbligato" anche verso gli altri titolari** che, a sua conoscenza, stanno trattando i dati oggetto della istanza di cancellazione.
Questa riforma, come è facile intuire, rappresenterà quindi un vantaggio notevole per i cittadini Europei.
Ai diritti testé analizzati, se ne aggiunge uno nuovo, che possiamo definire 3.0: la portabilità dei dati.
Seppure, a primo impatto, possa sembrare simile al diritto d'accesso, questo nuovo diritto ne condivide solamente le basi: il controllo da parte dell'interessato dei propri dati e la libertà di scegliere come e se farli circolare.
Infatti, questo innovativo diritto fornisce la possibilità in capo all'interessato di poter ricevere da un titolare del trattamento tutti i dati personali che lo riguardano in un formato strutturato, di uso comune, leggibile da dispositivo automatico, in modo da poterli all'occorrenza trasmettere agevolmente ad un altro fornitore di servizi o comunque ad altro titolare del trattamento.

In particolare, l'art. 20 del GDPR prevede che:

- ✓ l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti (qualora siano trattati sulla base del consenso preventivo dell'interessato oppure in esecuzione di un contratto di cui l'interessato è parte, ed il trattamento sia effettuato con mezzi automatizzati);
- ✓ nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile;
- ✓ tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- ✓ il diritto di cui al primo punto non deve ledere i diritti e le libertà altrui.

La possibilità di **trasmettere in maniera semplice e veloce i propri dati da un titolare all'altro**, risponde all'esigenza di poter agevolmente migrare da un servizio ad un altro senza che la "reputazione" acquisita fino a quel momento costituisca un impedimento**.**
La situazione tipica è la volontà dell'utente di passare ad un nuovo servizio telefonico, di somministrazione di luce, gas, acqua, servizi di posta elettronica, ma anche social network, cloud e, in generale, a qualsiasi servizio in cui l'aspetto reputazionale abbia una qualche rilevanza. D'altra parte, il diritto a che tale passaggio avvenga senza perdere quanto precedentemente acquisito o compiuto, costituisce la più piena realizzazione della libertà del consumatore in un mercato concorrenziale[35].
Oltre ad ampliare il margine di controllo dei consumatori impedendo forme di "*lock-in*"

[35] "Il diritto alla portabilità dei dati. Tra diritti della persona e diritti del mercato" di Andrea Giulia Monteleone

tecnologico, si prevede che il diritto alla portabilità dei dati promuoverà l'innovazione e la condivisione di dati personali fra titolari del trattamento in piena sicurezza e sotto il controllo dell'interessato.

5. GDPR: : solo compliance o una reale opportunità?

Una volta analizzate nel dettaglio le differenze tra il GDPR e la vecchia normativa, cerchiamo di capire se l'adempimento al nuovo Regolamento costituisce esclusivamente un mero onere di *compliance* oppure può essere interpretato come una vera e propria opportunità di sviluppo e quindi di creazione di valore per le imprese.

Per rispondere a questa domanda facciamo un passo indietro, e analizziamo un *asset* chiave per le organizzazioni.
Dopo avere elaborato una strategia, un'organizzazione, qualunque sia il suo *business*, deve stabilire quale struttura organizzativa sia in grado di realizzarla nel modo più efficiente, creando al tempo stesso un vantaggio competitivo sostenibile a lungo. È stato dimostrato che le persone agiscono, con maggiore o minore motivazione, anche in rapporto alla struttura organizzativa in cui operano, il che spiega i forti legami fra strategie e strutture.

Una struttura organizzativa dovrebbe avere almeno tre requisiti:

- ✓ anticipare l'evoluzione del settore e dell'ambiente (sviluppo dei mercati, progresso tecnologico, tendenze nella distribuzione);
- ✓ essere adatta alle scelte strategiche dell'impresa e alla sua posizione nell'ambiente competitivo;
- ✓ essere adatta alla cultura dell'organizzazione, alle capacità distintive della stessa e anche alle personalità dei manager di vertice.

Sono svariate le strutture organizzative che le imprese moderne, a seconda delle proprie esigenze, possono adottare. Le strutture organizzative, infatti, possono essere di tipo funzionale, divisionale, essere reticolari, ecc.; ma un punto chiave che accomuna tutte le diverse tipologie è la necessità di comunicazione tra diverse *business unit* per il raggiungimento di un obiettivo comune.
Nel tempo si è riscontrato quanto sia indispensabile investire sulle nuove tecnologie in maniera intelligente e versatile, per restare al passo con i tempi e non rimanere bloccati in investimenti vischiosi.
Discorso che risulta essere valido anche in ambito di comunicazione tra SBU (*Strategic Business Unit)* poiché lo sviluppo tecnologico, anche qui, costituisce un fattore differenziante.
L'impatto maggiore della trasformazione digitale però, si è verificato sulle *business unit* che si confrontano direttamente con il mercato e i clienti.
Le unità che riscontrano la necessità di mantenere uno stretto contatto con i clienti, infatti, devono capirne le esigenze, le abitudini, le scelte di fronte alle azioni dei competitor. Questo significa tenere traccia delle attività del cliente da quando è solo potenziale (*lead*) a quando sottoscrive un contratto e per tutta la durata dello stesso, oppure fino a quando decide di acquistare un determinato prodotto.
La tracciabilità sappiamo essere uno dei punti di forza dei dati, e, tramite la *digital innovation,* si può fare in modo che le informazioni acquisite da un canale di contatto risultino disponibili agli altri canali in maniera più e veloce e più mirata, riuscendo così a offrire

al cliente un servizio migliore a costi più bassi**.** Molto spesso però, tramite una ricerca frettolosa dei vantaggi competitivi dovuti ad una maggiore digitalizzazione, le organizzazioni hanno implementato procedure, infrastrutture tecnologiche sempre più aperte e connesse, ma in modo disordinato o disomogeneo, con forti lacune in area sicurezza.

Il GDPR in questo senso mette in ordine e riorganizza il sistema di sicurezza, curando e migliorando l'aspetto dell'automazione dei dati, dei processi e della sicurezza nella sua globalità. Infatti, grazie all'utilizzo degli innovativi strumenti inseriti nella normativa e precedentemente analizzati, la nuova direttiva tenta di fornire una nuova struttura organizzativa per il trattamento dei dati personali che, se attuata in modo corretto, potrebbe comportare numerosi vantaggi per le imprese.
Nell'organizzazione interna, tenere traccia dei trattamenti effettuati, dei rischi e dell'impatto che ne deriva, come imposto dagli artt. 30 e 35 del GDPR, dovrebbe tornare utile agli stessi soggetti che si occupano di sicurezza e che "mappano" anche dal punto di vista della privacy il *workflow*.

Un primo vantaggio, immediato, percepibile dalle PMI e dalle "*big companies*", è indubbiamente l'allontanamento delle sanzioni. Tuttavia, ci sono altri vantaggi non immediatamente fruibili.
Le crescenti richieste derivanti dai diritti di cui agli artt. 15 e ss. del GDPR sono un'occasione per adattare meglio anche le tecniche di recupero delle informazioni e dei dati in possesso delle aziende, nel momento in cui si tiene traccia dei trattamenti.
Questo significa ridurre il tempo di attesa tra richiesta (es. accesso ai dati) e risposta dell'azienda, la quale può dedicare maggiori risorse alla produttività, piuttosto che alla difesa dei diritti degli interessati (che, per quanto nobile, è un'attività che potenzialmente gravava già con la 196/2003 sulle aziende e richiede maggior rigore e impegno con il GDPR).

Le procedure imposte dal GDPR quindi, una volta assimilate, consentono di dedicare meno tempo agli adempimenti privacy e più tempo alla produttività.
Se ignorate o applicate in modo sporadico o disorganizzato, espongono a rischi e sottraggono personale dalle attività redditizie.
Questo è vero in particolar modo per le PMI, le quali probabilmente non destinano specifiche risorse a queste cause.
Il GDPR nasce considerando il panorama ormai incontrollabile di cyber attacchi e minacce, sempre più gravi, al patrimonio informatico e alla privacy di manager e imprese.
In un contesto sempre più connesso, dove IT e IoT entrano sempre di più nella vita di tutti i giorni, **sono i dati il punto di partenza di qualsiasi business, e come tale vanno protetti**.

Garanzia dei dati significa maggior fiducia da parte del cliente: dato che il GDPR impone che ogni nuovo servizio o processo aziendale che utilizza i dati personali deve prendere in considerazione la protezione dei medesimi prima della sua implementazione, le aziende devono essere in grado di garantire un determinato grado di sicurezza e dimostrare il costante monitoraggio della protezione dei dati.
Essere in grado di creare prodotti o servizi che facciano sentire al sicuro il cliente nell'usarli significa garantire il successo del business e costruire un rapporto di fiducia, attraverso una strategia di *governance* a 360 gradi.
Inoltre, **la figura del DPO assicurerà un "marchio di qualità**" in termini di organizzazione e di corretto trattamento dei dati per le imprese. Nominarlo, quindi, diventerà necessario anche per le imprese che non risultano essere obbligate a farlo, poiché verrà considerato un requisito essenziale dai clienti.

In altre parole, nell'intraprendere le proprie azioni per il GDPR, le organizzazioni devono focalizzarsi sul divario esistente tra il loro attuale sistema di gestione dei dati e quello che servirebbe per ricavare **concreti vantaggi di business dalle proprie informazioni**, in un'ottica di "*digital data transformation*".

Il DPO, quindi, viene considerato un presupposto di legittimità per l'adempimento al GDPR e, come più volte sottolineato, una nuova figura che avrà un ruolo molto importante per le aziende. Nella nomina del DPO il principio di *accountability* richiede di fare delle valutazioni interne in ordine alle caratteristiche aziendali e ai requisiti invece prescritti per legge dall'art 37 del regolamento.
A questo si aggiunga la questione, non secondaria per l'azienda, del costo che comporta la nomina della figura del DPO. E' chiaro che nel caso in cui fosse necessario rivolgersi all'esterno per assumere questo specialista, verrebbe alla luce un conseguente profilo di onerosità, ma, lasciando libera la possibilità di individuare questa figura all'interno dell'organizzazione, **il GDPR concede la facoltà alle aziende di contenere i costi tramite l'investimento in formazione interna**.

Le soluzioni sono quindi due: rivolgersi quindi al mercato esterno, laddove non siano immediatamente presenti all'interno dell'organizzazione le professionalità necessarie per garantire l'esercizio della funzione del ruolo, ovvero, tramite un approccio meno oneroso, investire su formazione interna, individuando il responsabile nell'ambito delle proprie strutture, con quelle attenzioni di incompatibilità messe bene in evidenza dal WP 29.

Dal punto di vista delle competenze professionali il **DPO** deve coniugare alla conoscenza della normativa, e quindi una capacità di natura giuridica, la pregressa consapevolezza e quindi padronanza delle conoscenze tecnologiche necessarie ad assicurare l'indirizzo nella protezione dei dati.
Per ricoprire questa complessa carica devono quindi coesistere questi due emisferi professionali.

Requisiti facilmente riscontrabili sulle offerte di lavoro presenti su LinkedIn che perlopiù richiedono:

- ✓ laurea (in legge o ingegneria gestionale o in economia aziendale);
- ✓ competenza sulle norme europee a presidio della *data protection*;
- ✓ precedente esperienza (almeno 4 anni) nella redazione di *privacy policies*;
- ✓ precedente esperienza (almeno 4 anni) nella implementazione di sistemi di controllo, *assessment* e mitigazione dei rischi;
- ✓ precedente esperienza (almeno 4 anni) nella gestione e analisi dei processi *IT Security*;
- ✓ ottime competenze e attitudini informatiche;
- ✓ ottime capacità comunicative (parlate e scritte) sia in italiano che in inglese, verso tutti gli stakeholders, dal CdA agli interessati, dai manager al dipartimento IT e legal;
- ✓ dimostrate capacità di rapporti con i clienti, al fine di un costante allineamento con titolari e responsabili del trattamento dei dati personali.

Aldilà delle conoscenze personali, però, il *Data Protection Officer* non è una figura che può rimanere isolata. Bisogna prevedere, soprattutto nelle grandi aziende, un ufficio del DPO, ovvero un *team* che possa sommare queste caratteristiche e coadiuvare il lavoro del responsabile della protezione dei dati.

LA SECURITY

1. Il Security Management

Il concetto di **security** ha conosciuto una rilevante evoluzione negli ultimi anni. Questa evoluzione è sintetizzata dalla norma UNI 10459 del sistema UNI EN ISO 9000 – 1[36] (norma di gestione per la qualità e di assicurazione della qualità), che definisce la security aziendale come "*studio, sviluppo e attuazione delle strategie, delle politiche e dei piani operativi volti a prevenire, fronteggiare e superare eventi in prevalenza di natura doloso e/o colposa che possono danneggiare le risorse materiali, immateriali, organizzative e umane di cui l'azienda dispone o di cui necessita per garantirsi un'adeguata capacità concorrenziale nel breve, nel medio e nel lungo termine*".

Quindi, accanto alla gestione delle variabili competitive tradizionali, l'azienda, sia essa industriale, bancaria, commerciale, finanziaria o altro, ha come obiettivo la tutela del suo patrimonio, inteso nell'accezione più vasta del termine (risorse materiali, immateriali e umane), che si pone alla base dei processi di creazione del valore aziendale, assicurando il mantenimento della capacità reddituale nel tempo.

Con la locuzione **security management** si indicano tutte quelle attività gestionali di individuazione, valorizzazione e analisi del rischio che può provocare danni patrimoniali e non (furti, frodi, divulgazione di informazioni, ecc.) ad un'azienda, ente o raggruppamento di beni e persone.

Racchiudendo il termine "sicurezza" molteplici eventi gestionali, è possibile distinguere tre diverse tipologie di security management, per ognuno dei quali viene individuato un responsabile della funzione:

- ✓ sicurezza patrimoniale: il Loss Prevention & Security Manager è il responsabile aziendale per la sicurezza patrimoniale. Si occupa di tutte le attività di vigilanza e di investigazione per far fronte alle perdite dell'azienda legate a furti, frodi o truffe;
- ✓ sicurezza informatica: l'IT Security Manager è colui che deve garantire la sicurezza dei sistemi informatici, al fine di renderli inattaccabili dall'esterno, predisponendo la relativa protezione delle informazioni e dei dati aziendali o da virus;
- ✓ sicurezza sul lavoro ed ambiente: il Responsabile della Sicurezza Aziendale è colui che deve garantire la vivibilità dei posti di lavoro, individuarne eventuali pericoli e trovarvi il giusto rimedio (Decreto legislativo 81/2008).

In ogni caso, l'attività di security management viene svolta secondo precise *items*, interessando settori ben definiti e con la condivisione di tutte le divisioni dell'azienda.

Tali *items* si possono riassumere come segue:

- ✓ valori aziendali: individuazione del campo di attività dell'azienda e riconoscimento dei responsabili delle varie strutture;
- ✓ definizione degli obiettivi:
  a) obiettivi strategici - non devono intralciare le strategie e le politiche aziendali;

[36] Sistemi di Gestione per la Qualità UNI EN ISO 9001/2000.

b) obiettivi operativi - devono essere efficaci ed efficienti sul piano attuativo delle primarie attività aziendali;
c) obiettivi di conformità - devono rispettare pienamente le leggi civili e penali dello Stato e/o i regolamenti aziendali;
d) obiettivi di reporting - devono essere assicurate una piena distribuzione e un'attività di informazione delle politiche da emanare;

- ✓ identificazione del problema: identificazione dei rischi;
- ✓ *risk assestment*: analisi dei rischi individuati precedentemente e valutazione del loro impatto, tenendo conto dei rischi potenziali e dei rischi effettivi;
- ✓ *risk response*: individuazione delle attività di contenimento e/o di contrasto da svolgere per la riduzione dei rischi analizzati;
- ✓ *control activities*: stabilire e rendere pubbliche le politiche, le attività, le procedure attuative;
- ✓ *information & communication*: attività di audit interno, divulgazione e spiegazione delle procedure emanate, al fine di renderle comprensibili a tutti coloro che sono tenuti ad applicarle;
- ✓ *monitoring*: attività di controllo continuo dell'applicazione delle procedure.

L'attività di security management, in generale, è ancora poco utilizzata all'interno delle aziende, poiché ritenuta un costo e non un investimento, ma fortunatamente il *trend* sta cambiando.
Il security management, nel rispetto della dottrina della scienza della sicurezza, deve essere in grado di presidiare rischi e minacce a tutto campo in relazione agli scenari sempre in evoluzione in ambito tecnico, informatico, economico, finanziario, in un contesto sempre più globalizzato ed interconnesso con le realtà più disparate.
La scienza della sicurezza è lo studio del rischio nelle sue varie forme, dirette ed indirette, con l'obiettivo di ridurlo fino ad annullarlo (difficilmente) o (meglio) controllarne le conseguenze; si parla di "riduzione" perché l'eliminazione del rischio è matematicamente impossibile, essendo le variabili infinite ed imponderabili.
È una materia multidisciplinare, alla quale fanno riferimento molte aree tematiche e diverse sotto-discipline: ogni area tratta un aspetto particolare della vita della persona, creando un insieme organico di cognizioni e di misure tali da produrre come risultato l'incolumità e il benessere (sicurezza) della persona, e di conseguenza della collettività.
A partire dall'analisi del rischio si perviene alla definizione di una prevenzione massima possibile: il cosiddetto rischio accettabile.
Poiché la sicurezza può interessare le azioni dell'uomo direttamente (ad esempio nell'ambito della difesa personale) oppure indirettamente (ad esempio i suoi interessi, come nell'ambito della sicurezza finanziaria), la scienza della sicurezza presenta numerose specializzazioni per potersi interfacciare nel migliore dei modi alle varie discipline correlate all'attività umana; la sicurezza, infatti, deve in ogni momento circondare la persona e i luoghi in cui si svolge ogni sua attività.
Per tale motivo possiamo parlare di sicurezza sportiva, relativa all'aspetto agonistico, sicurezza sanitaria, che analizza il mondo della medicina e della profilassi, sicurezza alimentare, che attiene al mondo del cibo e delle diete, dalla produzione al consumo, sicurezza stradale, specifica per tutto ciò che attiene le strade, i veicoli e la circolazione stradale, sicurezza informatica, che si attaglia all'uso delle reti telematiche in relazione all'uso che ne fa l'uomo, e poi ancora si parla di ingegneria della sicurezza che si occupa dei ritrovati scientifici e tecnologici al fine di rendere più sicura la vita quotidiana; sicurezza nucleare che si prefigge l'obiettivo di eliminare (*rectius* ridurre) i rischi associati all'uso dell'energia nucleare; sicurezza bancaria, che analizza il mondo degli investimenti e dalla Borsa.

Si tratta, evidentemente, di un'esemplificazione non esaustiva delle applicazioni della scienza della sicurezza, che però aiuta a capire quanto questa disciplina attenga a tutte le possibili variabili dell'esistenza dell'uomo, avendo sempre come fine quello di prevenire e proteggere da potenziali rischi l'uomo, sia nella sua individualità che nella sua socialità.

È purtroppo diffuso l'erroneo convincimento che la sicurezza sia sempre un compito degli "altri" (*in primis* - giustamente - dello Stato, poi delle Forze dell'Ordine, dei medici, ecc.), ma in realtà il primo responsabile per la propria e l'altrui sicurezza è l'individuo che è, al contempo, soggetto e oggetto della sicurezza.

2. Il ciclo della sicurezza

A livello internazionale il concetto di sicurezza, o meglio quella che nel nostro Paese definiamo con il termine "sicurezza", si esplica in tre diversi ambiti, ciascuno specificamente individuato.
Si parla infatti di:

- ✓ *safety*, intesa come tutela dell'incolumità della persona, dall'antinfortunistica alla sicurezza sul lavoro;
- ✓ *security*: intesa come cultura, studio e gestione della sicurezza per la realizzazione di misure per la prevenzione da azioni e comportamenti tesi a danneggiare l'individuo. Tali misure possono essere materiali e infrastrutturali, ma soprattutto formative ed informative, atte cioè a far conoscere il rischio e quindi ad evitare il pericolo;
- ✓ *emergency*: intesa come attività di protezione dal/contenimento del pericolo.

Ecco allora che da questa elencazione riassuntiva emergono alcuni concetti che possiamo definire "chiave" in materia di sicurezza, dai quali cioè non si può prescindere.

Vediamoli:

- ✓ **sicurezza**: conoscenza che l'evoluzione di un sistema in un dato senso non manifesti stati indesiderati;
- ✓ **rischio**: probabilità che si verifichi un dato evento, caratterizzato da una determinata gravità del danno sulle persone, sulle cose e/o sull'ambiente;
- ✓ **pericolo**: proprietà intrinseca di una sostanza, di un'attrezzatura di lavoro o in generale di un evento, avente potenzialità di creare danno;
- ✓ **analisi**: studio della statistica, dell'ambiente interessato, delle persone che operano e dell'attività che vi si svolge, al fine di realizzare una valutazione del rischio;
- ✓ **prevenzione**: messa in opera di tutte le misure derivate dall'analisi, per evitare che si realizzino eventi pericolosi (e quindi dannosi);
- ✓ **protezione**: messa in opera ed in esercizio di tutte le misure per proteggere persone e cose dal rischio residuo. Può essere collettiva (prioritaria) o individuale, attiva o passiva;
- ✓ **gestione**: insieme di attività che si realizzano in fase sia di normale esercizio che in emergenza. La gestione in normale esercizio è quell'insieme di attività quali la formazione, l'informazione, le manutenzioni, le verifiche, le esercitazioni, gli adeguamenti normativi e le procedure; la gestione in emergenza è la messa in atto delle protezioni manuali, quindi le evacuazioni, le chiamate di emergenza, il contenimento, lo spegnimento, il confinamento e l'allontanamento.

Individuati i concetti chiave, è necessario ora soffermarsi sui criteri generali che devono informare una corretta attività di sicurezza.
Il primo criterio è rappresentato sicuramente dalla conoscenza: la percezione del rischio, sia personale che ambientale, l'analisi del contesto operativo. E' proprio dall'inconsapevolezza, dal non conoscere e dal non avere la giusta percezione del rischio che nasce l'errore, inteso come situazione di rischio.
Segue, evidentemente, il rischio e quindi la necessità di un'analisi del rischio che dia la possibilità di creare un piano di prevenzione che consenta di ridurre, contenere o evitare i danni. La conoscenza e la coscienza del rischio sono il primo passo verso la sicurezza.
Spesso sappiamo che esiste un rischio perché ci è stato detto, ma manca la percezione e la coscienza del "rischio reale"; per fare un esempio, si può dire di non mettere la mano sul fuoco ai bambini, ma se almeno una volta non ne fanno esperienza, difficilmente ne avranno la giusta percezione e coscienza. Ci sono al contrario delle esperienze irreversibili come gli incidenti stradali, per le quali non si può provare (fare esperienza), ad esempio, a correre guidando in stato di ebbrezza per essere coscienti del rischio reale, perché il danno fisico, sociale, morale, economico che ne deriverebbe potrebbe essere irrecuperabile.
La "percezione del rischio" coinvolge dei meccanismi di tipo psicologico: in genere la mente umana tende a valutare come "più rischiose" le situazioni che hanno una maggiore gravità (ovvero le situazioni che possono provocare la morte), e "meno rischiose" le situazioni a cui è associata una gravità minore (ad esempio le situazioni che possono provocare un danno fisico non irreversibile).
Un altro meccanismo psicologico che altera la percezione del rischio è quello per cui generalmente si valutano come meno rischiose le condizioni di cui si ha il controllo: ad esempio, in genere una persona tende ad essere meno preoccupata se è la persona stessa a guidare rispetto alla situazione in cui l'autista è una persona diversa.
La scienza della sicurezza quindi non deve tenere conto della percezione del rischio, ma del rischio reale.

Abbiamo così a disposizione gli elementi per fissare quello che viene definito il "ciclo della sicurezza", ovvero un ciclo virtuoso che parte dall'analisi, cioè dallo studio legislativo, normativo, ambientale, personale, professionale, delle attività e dei processi.
All'analisi conseguono le misure, divise nei due macro insiemi di prevenzione e protezione. Le misure possono essere attive, passive, strutturali, impiantistiche, amministrative o disciplinari e servono a realizzare il fine di sicurezza che ci si è posti.
Ma, una volta che le misure di sicurezza sono state individuate ed attuate, si rende necessario mantenerle efficaci. E' la parte detta della gestione che mira mantenere in vita il livello di sicurezza raggiunto, attraverso studi, aggiornamenti, formazione, informazione, manutenzione, verifiche, esercitazioni, piani di sicurezza e adeguamenti.

Un sistema sicuro non è un sistema chiuso, bensì funziona e migliora se dispone di solide basi tecniche e normative e di costante confronto con altre realtà.

3. Gli standard internazionali

L'attività di normazione consiste nell'elaborare documenti tecnici che, pur essendo di applicazione volontaria, forniscano riferimenti certi agli operatori e possano pertanto avere una chiara rilevanza contrattuale.
A volte l'argomento trattato dalle norme ha un impatto così determinante sulla sicurezza del lavoratore, del cittadino o dell'ambiente che le Pubbliche Amministrazioni fanno rife-

rimento ad esse richiamandole nei documenti legislativi e trasformandole, quindi, in documenti cogenti. In ogni caso, a mano a mano che si diffonde l'uso delle norme come strumenti contrattuali e che, di conseguenza, diventa sempre più vasto il riconoscimento della loro indispensabilità, la loro osservanza diventa quasi "imposta" dal mercato.
In tale contesto è evidente che l'attività normativa nazionale si sta progressivamente limitando a temi più specificatamente locali o non ancora prioritari per studi sovranazionali, mentre investe sempre maggiori risorse per contribuire alle attività europee ed internazionali.

L'attività di normazione ha per oggetto anche la definizione dei processi, dei servizi e dei livelli di prestazione, nonché la definizione degli aspetti di sicurezza, di organizzazione aziendale (UNI EN ISO 9000) e di protezione ambientale (UNI EN ISO 14000), così da tutelare le persone, le imprese e l'ambiente.

Particolarmente interessate rispetto al tema trattato è la **norma UNI 10459**, che disciplina la **Security** e la figura professionale del **Security Manager**. Infatti, nel sistema della vigilanza privata, tale norma assume particolare vigore - unitamente alla norma UNI 10891, che regola la qualità dei servizi degli istituti di vigilanza privata - perché resa cogente dal Decreto del Ministro dell'Interno 1 dicembre 2010, n. 269, in materia di capacità tecnica e qualità dei servizi degli istituti di vigilanza.

4. Una security sostenibile

La security, quindi, nell'ambito delle competenze attribuitegli allo scopo di tutelare da minacce esterne il personale, gli asset societari, le informazioni e il know-how dell'azienda, deve analizzare e implementare le soluzioni più idonee, di tipo sia organizzativo che tecnologico, nel pieno rispetto dei principi di sostenibilità in ambito nazionale ed estero.
Come abbiamo visto, l'aggiornamento costante delle condizioni di security in tutte le realtà operative aziendali, l'adozione di adeguate misure protettive e la gestione delle opportune iniziative di comunicazione, in coordinamento con quelle logistiche a supporto del personale e dei familiari, rappresentano, dunque, l'obiettivo primario del complesso delle attività di security.
Gli indicatori di criticità continuano a disegnare scenari che potrebbero avere diretta incidenza sugli ambiti aziendali, e il personale operante nei paesi cosiddetti a rischio può essere tra gli obiettivi di questa minaccia. L'impatto di eventuali azioni contro tali interessi figura nelle agende internazionali, dove si cerca, in un'ottica collaborativa, una maggiore sinergia tra pubblico e privato con l'obiettivo di mitigare i rischi inerenti a quelle che possono essere considerate infrastrutture critiche nazionali. È in tale quadro che viene rafforzata con sistematicità la collaborazione con le entità statuali preposte alla sicurezza, in Italia ed all'estero, per rafforzare e migliorare il dispositivo di reazione rispetto alle tipologie di eventi che possono compromettere la stabilità del business, l'integrità delle persone e la sicurezza delle infrastrutture.

La **partnership pubblico-privato** (**PPP**) è uno dei temi fondamentali su cui si sono impegnate le principali agenzie internazionali che operano nell'ambito della sicurezza. La sua importanza nella lotta al terrorismo è stata chiaramente rilevata nel documento che fissa la strategia globale delle Nazioni Unite contro il terrorismo (The United Nations Global Counter - Terrorism Strategy, 2006). Sulla base di ciò, l'UNICRI (l'Istituto di Ricerca per il Crimine Internazionale e la Giustizia delle Nazioni Unite) e l'OSCE (Organizzazione per la Sicurezza e la Cooperazione in Europa) hanno dato vita ad un progetto congiunto volto a promuo-

vere la collaborazione fra le aziende private e il settore pubblico; il predetto progetto ha come settore di riferimento le infrastrutture critiche che producono energia non nucleare. La partnership fra il pubblico e il privato promossa dall'OSCE e dall'UNICRI è volta primariamente allo scambio di quelle informazioni che sono vitali per la prevenzione di attentati terroristici diretti contro le predette infrastrutture critiche e che possono migliorare le risposte e gli interventi in caso di attacco.

In questo contesto, nell'ottica promossa dall'OSCE e dall'UNICRI, la figura del **Security Manager** viene individuata come quella più indicata per interloquire con gli organismi pubblici - nazionali e internazionali - al fine di instaurare la partnership di cui sopra. Essendo parte integrante della struttura aziendale, costui è in grado di comunicare all'esterno le problematiche più rilevanti cui deve fare fronte l'impresa privata, e quindi di indirizzare il legislatore e gli apparati dello Stato nei processi decisionali e nell'adozione delle più efficaci strategie per la tutela del patrimonio aziendale del Paese. Tuttavia, il Security Manager ha anche le conoscenze tecniche necessarie per comprendere appieno le informazioni provenienti dalle agenzie pubbliche, per poterle valutare efficacemente e per attuare le azioni opportune e adeguate in base al contesto di riferimento. Sono infatti definiti una serie di processi e di scambi informativi di dati sensibili che possono essere gestiti solo da un professionista della sicurezza riconosciuto come tale, che sia in grado di parlare lo stesso "linguaggio" dell'Autorità pubblica.

L'obiettivo di mitigazione del rischio, in linea con i principi di sostenibilità, ha reso pregnanti anche per la security alcuni principi che sono divenuti fondanti, quali il rispetto dei diritti umani e delle best practices internazionali. L'adesione ai *Voluntary Principle for Security and Human Rights* rappresenta una delle azioni in cui assume particolare valenza una corretta gestione della security.
Questi articolati obiettivi e questi continui richiami delle norme delimitano un perimetro che, in aderenza agli standard internazionali, ravvisa forte la necessità di coniugare in un unico ambito specializzato gli aspetti concernenti la security. È ormai diffusa la percezione che, negli ultimi anni, ci siano stati drammatici e profondi cambiamenti nella natura del contesto imprenditoriale e nella società in generale. In particolare è stato detto, quasi fino alla nausea, che il mondo è cambiato a partire dall'11 settembre 2001.

Tuttavia, molti di questi 'nuovi cambiamenti' hanno semplicemente evidenziato i problemi che le aziende e le comunità hanno affrontato per diversi decenni. È quindi emersa l'imperativa esigenza di considerare questioni che, in precedenza, non facevano parte della coscienza collettiva. Come società siamo stati informati della necessità e dell'esistenza di misure di sicurezza. Quando la sicurezza ha a che fare con la vita lavorativa ordinaria, però, viene spesso vista come un ostacolo alla routine quotidiana.
Gli atteggiamenti sono comunque cambiati notevolmente negli ultimi tempi, concentrandosi su una maggiore attenzione alla sicurezza. Eppure, questo cambiamento negli atteggiamenti è spesso guidato da un'errata percezione, alimentata dai media che a volte diffondono una visione eccessivamente drammatica del contesto di riferimento. Il risultato è che gli investimenti sulla sicurezza potrebbero essere erroneamente indirizzati dove c'è "caos informativo" e non dove è veramente necessario che siano impiegati.

Una migliore comprensione della natura del rischio favorisce un processo decisionale più informato, aumenta le capacità di sfruttare le opportunità e riduce i danni. Tradizionalmente, l'industria della sicurezza e l'attenzione delle professioni a rischio si sono concentrate sulla minimizzazione del rischio stesso, con attività finalizzate alla prevenzione degli infortuni, senza tuttavia necessariamente considerare a fondo la natura e il livello del

pericolo. Oggi, invece, bisogna fornire alle aziende i mezzi per assumere decisioni ragionate sulla necessità di migliorare la sicurezza e di utilizzare appropriatamente il proprio budget e le altre risorse per investire in essa.

Nella sua forma più sostanziale, la security si concretizza nella capacità di fornire la struttura e i mezzi per determinare la natura delle minacce, tracciare il "corso delle vulnerabilità", comprendere le potenziali conseguenze di eventi futuri, e sviluppare un approccio più strategico per tali attività. Questo approccio è nato per considerare le cause profonde, le pressioni dinamiche e le condizioni pericolose.

Il **Security Manager** deve saper cogliere nella sua analisi dinamica ed olistica le cause profonde, quali ideologie basate su diversi sistemi politici, economici e sociali, negazione dei fondamentali diritti umani e della libertà, aumento della conflittualità sociale e della discordia; pressioni dinamiche quali la mancanza di istituzioni governative, sociali e locali; ostacoli alle capacità di sviluppo, alle opportunità d'impiego e ai livelli d'investimento; condizioni pericolose, come un ambiente fisico fragile, segmentato da zone pericolose, con edifici non protetti e infrastrutture deboli, condizioni economiche locali variabili, incapacità di gestire le emergenze.
È in tali ambiti che bisogna implementare la comunicazione e la consultazione con gli stakeholder interni ed esterni, saper determinare il contesto, strutturare le attività, sviluppare criteri di valutazione. Avere le conoscenze per poter identificare i rischi, determinare le minacce, individuare gli elementi critici, organizzativi e collettivi, determinare la vulnerabilità di tali elementi alle minacce individuate, identificare specifici eventi e scenari e le loro possibili conseguenze. Saper effettuare una analisi del rischio in grado di valutare i controlli esistenti, determinare le conseguenze derivanti dal concretizzarsi del rischio, determinare le probabilità che da un tale rischio scaturiscano specifiche conseguenze, definire il livello di rischio su una combinazione di conseguenze e probabilità. Ed inoltre poter effettuare una valutazione del rischio per determinarne la tolleranza e l'eventuale necessità di ulteriori trattamenti. Stabilire le raccomandazioni e le strategie per il trattamento dei rischi prioritari, assegnare le responsabilità e verificare l'adeguatezza dei fondi necessari per le attività di trattamento dei rischi per poi iniziare il ciclo di controllo e revisione finalizzato al rilevamento di eventuali cambiamenti. Revisionare i rischi e le rispettive strategie di trattamento, monitorare e revisionare i progressi compiuti e i risultati di ciascuna delle fasi del processo.
Stiamo parlando di quella cultura aziendale in grado di valutare le strutture e i processi che sono diretti verso la massimizzazione dei benefici e la minimizzazione degli svantaggi in materia di security, compatibilmente con il raggiungimento degli obiettivi di business. Laddove security si definisce come la preparazione, la tutela e la protezione delle persone, dei beni e delle informazioni sia materiali che immateriali.
L'efficace gestione del rischio security è un requisito fondamentale con cui le aziende, gli individui e chi è incaricato della tutela delle nostre comunità devono ora operare.
C'è poi naturalmente una vasta gamma di rischi interni ed esterni all'azienda, agli individui o alla comunità, che vanno al di là delle preoccupazioni relative alla sicurezza. Tuttavia, il rischio security rappresenta una fonte di preoccupazione per i governi, i datori di lavoro, i dipendenti e i cittadini.
L'identificazione del rischio, elemento centrale del processo di *risk management*, riguarda la selezione chiara e ragionevole delle fonti dei rischi e degli eventi che possono potenzialmente avere un impatto sugli obiettivi delle persone, dell'azienda o della comunità. L'identificazione del rischio può essere affiancata dalla considerazione che le conseguenze di approcci più tradizionali come la minaccia, la criticità, la vulnerabilità, possono comunque essere contributi preziosi per il processo di identificazione. Il processo

infatti, sarà più completo una volta sintetizzate queste informazioni, anche se l'identificazione del rischio è molto più di una semplice valutazione separata della minaccia, della criticità e della vulnerabilità.

I termini "minaccia" e "rischio" sono di solito utilizzati alternativamente. Tuttavia, "rischio" non è sinonimo di "minaccia", e anche se i due termini alla fine sono correlati, in realtà sono molto diversi. In molte circostanze una minaccia sarà fonte di uno o più rischi. L'interazione della minaccia con qualcuno o con qualcosa, in un preciso momento, o dopo il trascorrere di un certo periodo di tempo, determinerà un rischio. Le minacce possono esistere, ma non necessariamente rappresentano un rischio.
L'esame del contesto di security, e le considerazioni sulle valutazioni della minaccia, criticità e vulnerabilità, permetteranno di identificare i potenziali rischi. I rischi dovrebbero essere descritti e analizzati nel modo più completo e dettagliato possibile, così da permettere al management di comprendere appieno la situazione.

Il rischio appare come "la possibilità che accada qualche cosa che possa avere un impatto sugli obiettivi": è una definizione molto importante perché esprime la crescente maturità nel considerare i rischi che si sono concretizzati negli ultimi tempi. L'applicazione di questa definizione allo svolgimento di una professione inerente alla sicurezza dovrebbe sollecitare a non identificare il rischio solamente con la minaccia, ma a inquadrarlo in una nozione molto più ampia.

Le cause profonde, alle quali si è fatto riferimento in premessa, possono essere relative a tematiche storiche come il fondamentalismo islamico, le percezioni anti-islamiche, le convinzioni dell'esistenza di cambiamenti nelle democrazie occidentali, le percezioni di un dissesto economico. Da queste cause profonde possono poi sorgere ed innestarsi altri fattori causali come l'antagonismo nei confronti del pensiero occidentale, l'ingiustizia dei regimi governativi occidentali, l'impotenza culturale nei confronti di culture sempre più dominanti.
Questi fattori hanno portato alla creazione di ideologie fondamentaliste, di comportamenti e strutture che diventano minacce o fonti di rischio. Per esempio, la nascita di gruppi islamici come Al-Qaeda, o Jemaah Islamiyah, la costituzione dell'Intifada nei territori palestinesi, il fallimento di società funzionanti o dell'ordine pubblico, in zone come la Somalia, il Sudan, la Sierra Leone, l'Iraq, l'Afghanistan, Papua Nuova Guinea, le Isole Salomone, il Congo, la Colombia, il Nepal.
Da queste fonti nasce il rischio, come un attacco mirato a immobilizzare una struttura critica, attacchi saltuari contro la popolazione locale finalizzati a creare il panico e la perdita di fiducia nelle istituzioni, o attacchi (omicidio o rapimento) finalizzati a rimuovere gli elementi chiave del management o i tecnici dell'azienda. Ciascun rischio dà vita ad una serie di potenziali conseguenze. Se uno dei suddetti rischi dovesse verificarsi - l'evento - allora una o più conseguenze potrebbero prodursi.

L'identificazione del rischio consiste quindi nel comprendere la natura della minaccia (la fonte di rischio), interagendo con importanti elementi come ad esempio la comunità, gli assetti aziendali (la cui importanza è espressa attraverso la criticità), e in che modo la natura di questi elementi può facilitare o inibire questa interazione (espressa attraverso la vulnerabilità). Le informazioni sul contesto, sviluppate nella fase iniziale del processo, forniscono un ideale punto di partenza per individuare la minaccia e il rischio. Tuttavia, questi elementi potrebbero comunque non fornire i dettagli sufficienti per ottenere un'individuazione ed un'analisi completa. Un'attività di ricerca più dettagliata potrebbe pertanto essere richiesta per sviluppare un'affidabile individuazione del rischio.

È importante che i dati e le fonti di informazioni siano affidabili e accurati, al fine di fornire l'analisi e la successiva decisione avendo appropriati punti di riferimento e ponderazione. La valutazione della criticità (il risk assessment), coinvolge l'individuazione degli asset critici (le persone, le proprietà, le informazione e i processi che li supportano), i quali potrebbero essere esposti o danneggiati dalla minaccia. La valutazione della criticità è un passo vitale per l'identificazione del rischio poiché fornisce il punto di partenza per considerare le minacce pertinenti e la vulnerabilità dell'azienda, della comunità o degli individui, a tali minacce. In molte circostanze sarebbe difficile e costoso condurre una dettagliata valutazione del rischio per ogni bene, luogo e persona. La valutazione della criticità consente di concentrare l'analisi su quegli asset ritenuti di maggior importanza per l'azienda, per la comunità o per l'individuo.

Si tratta in pratica di una funzione trasversale ad elevata specializzazione che percorre orizzontalmente l'azienda raccogliendo e sistematizzando le norme che presiedono alla funzione e ridistribuendole all'interno dell'azienda in un ciclo continuo di verifica e controllo a soddisfacimento degli stakeholder e degli interessi aziendali coniugando l'eticità dell'impresa in aderenza al principio costituzionale di utilità. Tra l'altro le norme sopra richiamate, oltre al minimo comun denominatore di poter essere considerate per la loro atipicità rispetto al mondo del lavoro e dei doveri a capo del datore del lavoro, parlano tutte di valutazione del rischio e di piani di sicurezza. Appare pertanto evidente che tutte devono inquadrarsi nella loro unitarietà ed unicità in un contesto di Security Risk Management perfettamente illustrata e dettagliata dalla sopra richiamata norma AS HB 167:2006.

IL SECURITY MANAGER

1. Il Security Manager

Il **Security Manager** è la figura di riferimento per l'organizzazione, la gestione e l'assunzione di responsabilità della sicurezza di un'azienda.
Deve, quindi, possedere una buona conoscenza del *business* dell'azienda in cui opera, delle tecniche per garantire la sicurezza fisica, la privacy e la *governance,* ed essere una figura di riferimento in grado di operare nell'azienda in modo trasversale, fornendo supporto all'interno e curando la comunicazione verso i terzi. Importantissima per quest'ultima, la capacità di gestire un partenariato pubblico-privato a tutto campo.

In una visione moderna della sicurezza, l'attività del Security Manager abbraccia un contesto molto ampio, che va dalla sicurezza fisica dell'infrastruttura, al controllo della protezione delle strategie produttive dell'impresa, alla sicurezza delle infrastrutture critiche, informatica e sul lavoro, ma anche alla fedeltà dei dipendenti, alle rete di informazione-comunicazione, all'introito delle merci, al trasporto protetto e sicuro dei prodotti, alla tutela della privacy (anche se oggi, come abbiamo visto, esiste una figura professionale dedicata) e molto altro.

Tra le numerose competenze del Security Manager, quella di *risk management* riveste sicuramente un'importanza primaria. Si tratta dell'analisi del rischio globale attraverso l'esame degli scenari, l'identificazione e valutazione del rischio, l'individuazione ed attuazione della giusta strategia di gestione e controllo, nonché l'utilizzo degli adeguati strumenti di controllo.

Il punto di partenza dell'attività è, come detto, l'esame dello scenario di riferimento, ovvero la valutazione e presa in carico del rischio, da quello fisico a quello strategico, l'esame dei riferimenti normativi, la strutturazione della funzione della security e le sue relazioni interne ed esterne, la collocazione organizzativa nonché la missione ed il ruolo della funzione di security.
Rientra in questo campo l'attività preliminare di *intelligence*: analisi del territorio, dell'azienda, del contesto competitivo, delle vulnerabilità, delle tipologie di rischio, delle opzioni di security nonché delle tecnologie di supporto.

Altra competenza del Security Manager è la funzione di governo della security: impresa e qualità, certificazione dei sistemi e delle professionalità, le norme ISO 150 9000 e loro evoluzione, il sistema della gestione aziendale secondo le norme UNI EN ed ISO, la security nei contratti esterni e nella sicurezza privata, la selezione, l'utilizzo e la gestione dei servizi di sorveglianza, l'organizzazione della sicurezza pubblica e privata, la definizione di una *security policy*, la sicurezza del *top management*, la tutela del patrimonio informativo.

Vi è poi la responsabilità per la sicurezza delle informazioni, nonché, la gestione delle relazioni istituzionali.
Quest'ultimo rappresenta uno degli aspetti più delicati fra tutte le competenze del Security Manager, cui è richiesta la capacità di alimentare costantemente il rapporto pubblico-privato, tendendo al modello del partenariato.

Nel corso degli anni lo Stato ha dovuto misurarsi con la difficoltà sempre crescente di far fronte all'esigenza di tutela della collettività e delle città e di sicurezza dei cittadini dai fenomeni criminali, particolarmente presenti in alcune regioni del Mezzogiorno d'Italia ma lentamente e progressivamente sviluppatisi ormai in ampie zone del Centro e Nord Italia.
Per il raggiungimento di questo risultato lo Stato ha dovuto ammettere e regolare il concorso degli enti locali e dei soggetti privati in alcune attività (definite "sussidiarie") volte, appunto, a garantire appieno e compiutamente la sicurezza dei cittadini.
In linea generale, già con la Direttiva Generale del Ministero dell'Interno per l'anno 2004, si prefigurava un sistema coordinato di sicurezza all'interno del quale le forze di polizia presenti sul territorio dello Stato, organi specificamente preposti alla sicurezza pubblica "primaria", fossero affiancate da soggetti privati, in particolare gli istituti di vigilanza privata, particolarmente rilevanti sotto il profilo della "prevenzione" per il raggiungimento degli scopi di pubblica sicurezza.
Tutto ciò, peraltro, in linea con quanto si registra in altri Paesi dell'Unione Europea laddove si tende a valorizzare il concetto di sussidiarietà, in materia di sicurezza dei cittadini, attraverso ampie deleghe al ruolo e alle funzioni del "privato" (ovviamente sempre entro il perimetro di regole generali e controlli di merito tracciato dallo stato di riferimento), al fine ultimo di coniugare nel migliore dei modi il concetto di "efficienza" con quello di "efficacia".

In tale ottica il Security Manager dovrà tenere conto delle conseguenze dell'impatto che l'attività dell'azienda può avere sul territorio e sulla popolazione. A seconda dei casi dovrà relazionarsi e collaborare con le forze di polizia, gli istituti di vigilanza privata, gli uffici pubblici connessi con l'attività aziendale, gli organi di informazione (stampa, redazioni on-line, radio e televisioni) e talora anche con servizi di informazione e sicurezza italiani o stranieri, ufficialmente contattabili - questi ultimi - attraverso i canali ambasciate-consolati.

Per far fronte a tutti gli aspetti sopra indicati, l'esperto della sicurezza (Security Manager) deve avere competenze indubbiamente vaste e di natura eterogenea, anche dal punto di vista tecnico-specialistico.
In generale, indipendentemente dal titolo di studio, il Security Manager deve possedere competenze e/o conoscenze tecniche, giuridico-legali e di criminologia, con riferimento specifico ai crimini informatici e alla tutela delle informazioni, nozioni sul rischio e sulla protezione aziendale, sulla tutela di marchi e brevetti, in materia di frodi aziendali, buona conoscenza di Internet e delle problematiche, dirette e indirette, ad esso afferenti (server, reti e periferiche, piattaforme hardware e software, commercio elettronico, ecc.), familiarità con i più diffusi protocolli di comunicazione e linguaggi di programmazione, oltre alla padronanza della lingua inglese, alla capacità di lavorare in team e alla disponibilità ad orari flessibili.
È ritenuto fondamentale, inoltre, un orientamento al *problem solving* e la capacità di imporre i necessari provvedimenti di sicurezza elaborati; spesso, infatti, è proprio il cliente del Security Manager ad ostacolarne il lavoro, magari inconsapevolmente.

Infine, quattro sono le "regole auree" del buon Security Manager: correttezza, trasparenza, riservatezza e comunicazione.
La correttezza si declina in capacità di non creare falsi allarmismi, per poi fingere di risolverli.
La trasparenza si traduce nella necessità di tracciabilità oggettiva di tutti i processi e disponibilità ai controlli interni. Riservatezza significa saper tutelare solo le informazioni critiche, lasciando tutto il resto alla disponibilità di tutti.

La comunicazione è un aspetto fondamentale della gestione della sicurezza, sia all'interno che all'esterno dell'azienda, e incide sulla buona riuscita dell'attività. Questo assunto è particolarmente evidente in caso di gestione di un'emergenza: vi è, da un lato, la necessità di comunicare in tempo reale, rapido, tanto più rapido quanto più grave è l'emergenza manifestatasi; dall'altro l'esigenza di attendibilità della comunicazione, quindi di scambio di dati che siano credibili, su cui poter lavorare e operare delle scelte.

La complessità delle competenze e delle conoscenze richieste, unita alla grande attualità delle problematiche inerenti la sicurezza, ha fatto si che in Italia, in questi ultimi anni, venissero realizzati corsi universitari e non a tema[37].
Negli Stati Uniti d'America e nel nord dell'Europa il ruolo e l'importanza nella strategia dell'azienda dell'esperto della sicurezza sono da tempo riconosciuti e sfruttati; in Italia il mercato sembra essere in espansione[38], facilitato anche da una certa flessibilità nell'inquadramento del Security Manager, che può operare come consulente all'interno di un'azienda, come libero professionista, o far parte di un'impresa che si occupa proprio di garantire questo tipo di servizio.

2. Il ruolo del Security Manager nella sicurezza delle informazioni

La disciplina che previene, gestisce e interviene nei problemi inerenti la perdita, la manomissione o il furto di dati prende il nome di *Disaster Recovery*, e si è evoluta ed ampliata fino ad abbracciare tutte le aree dell'organizzazione e a diventare *Business Continuity Management*.
La *Disaster Recovery* prende in considerazione le misure tecnologiche e logistiche organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'organizzazione per la gestione della propria attività.
A ben vedere, anche nel Codice dell'Amministrazione Digitale, che è uno dei documenti importanti per il *Business Continuity Plan*, esiste una definizione del *Disaster Recovery*. Il Codice dell'Amministrazione Digitale (CAD), emanato con il Decreto legislativo 7 marzo 2005, n. 82, costituisce un corpo organico di disposizioni che presiede all'uso dell'informatica come strumento privilegiato nei rapporti tra la pubblica amministrazione italiana e i cittadini dello Stato.
Emanato a seguito della delega al Governo contenuta all'art. 10 della Legge 29 luglio 2003, n. 229 (legge di semplificazione 2001), è entrato in vigore il 1° gennaio 2006, ed ha lo scopo di assicurare e regolare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale, utilizzando, con le modalità più appropriate, le tecnologie dell'informazione e della comunicazione all'interno della pubblica amministrazione, nei rapporti tra amministrazione e privati e, in alcuni limitati casi, disciplina anche l'uso del documento informatico nei documenti tra privati.
Nel 2006, pochi mesi dopo l'entrata in vigore, il Codice è stato oggetto di una serie di correttivi, disposti con il Decreto legislativo 4 aprile 2006, n. 159, la cui emanazione era stata autorizzata dalla medesima legge-delega n. 229 del 2003. Il decreto correttivo, oltre a modificare in diversi punti l'articolato del Decreto legislativo n. 82/2005, traspone nel *corpus* del Codice l'intero testo già contenuto nel Decreto legislativo n. 42 del 2005 (contestualmente abrogato), disciplinante il Sistema pubblico di connettività e la Rete

[37] A titolo di esempio basti pensare che l'Università di Bologna, Facoltà di Scienze Politiche, o l'Università di Roma Tor Vergata, Facoltà di Giurisprudenza, o ancora l'Università Telematica di Roma Niccolò Cusano, hanno istituito corsi di perfezionamento in Security Management e Security Manager).

[38] Isfol - elaborazione editoriale - 27.07.2010.

Internazionale delle Pubbliche Amministrazioni.
La disposizione originaria è stata più volte modificata, da ultimo con il Decreto legislativo 26 agosto 2016, n. 179 (c.d. CAD 3.0)[39].

Il *Disaster Recovery* è l'insieme delle misure tecniche organizzative adottate per assicurare all'organizzazione il funzionamento del Centro Elaborazione Dati, delle procedure e delle applicazioni informatiche dell'organizzazione stessa in siti alternativi a quelli primari di produzione, a fronte di eventi che possano provocare indisponibilità prolungate. Il *Disaster Recovery* è quindi l'insieme delle modalità con cui intervenire e difendersi nel caso di problemi ai sistemi informatici.

Il disastro è la conseguenza o l'effetto di una minaccia di un evento dannoso sulle attività dell'organizzazione, e può essere di tipo naturale, come un terremoto, uno tsunami, un tornado, un'alluvione, un'abbondante nevicata o l'eruzione improvvisa di un vulcano, ma può anche essere dovuto all'uomo o alle tecnologie, come nel caso di incendi, esplosioni, rotture di condutture dell'acqua, interruzioni elettriche o back-out, interruzione del servizio di linee di comunicazione e attentati terroristici.
Pensiamo poi ai gruppi di hacker che, sparsi per il mondo, stanno dando del filo da torcere alle più importanti organizzazioni, comprese quelle militari.

Un principio basilare va sempre tenuto presente: i disastri possono accadere, anche se remoti e con probabilità bassissime.

Nel contesto del *Disaster Recovery* il Security Manager deve garantire e salvaguardare il patrimonio di un'azienda e l'organizzazione produttiva che è definita all'interno dell *Business Continuity Management*.
Anche le informazioni sono patrimonio aziendale dell'organizzazione. L'anagrafica clienti è il cuore di un'azienda, e costituisce quindi un importantissimo patrimonio da proteggere, anche perché è l'asset più fragile, il bene più vulnerabile, poiché si tratta di dati che possono essere persi, rubati o manipolati, e finire nelle mani sbagliate.

Il *Disaster Recovery*, come elemento del *Business Continuity Management*, ha la sua affinità con il *Security Management*. Infatti, proprio la citata norma UNI 10459 stabilisce che una delle attività principali da svolgere è la valutazione della security delle informazioni, ossia l'*Information Security Assessment*, cioè la valutazione dei rischi di manipolazione e distruzione dei dati e delle contromisure necessarie.

Nel *Disaster Recovery Plan* il Security Manager disciplina tutte le procedure e le metodologie per attivare il *Disaster Recovery*, identificando i criteri per riconoscere una condizio-

[39] L'art. 16 del decreto anti-crisi (decreto legge n. 185/2008, convertito in legge n. 2/2009) ha modificato i commi 4 e 5 dell'art. 23, prevedendo per la copia firmata digitalmente lo stesso valore dell'originale senza obbligo di autentica da parte di notaio o di altro pubblico ufficiale, salvo i documenti da indicare con decreto del presidente del Consiglio dei ministri. Altre modifiche sono state introdotte dalla legge 18 giugno 2009, n. 69, e dalla legge 3 agosto 2009, n. 102. Successivamente, importanti modificazioni e integrazioni sono state introdotte dal decreto legislativo 30 dicembre 2010, n. 235. Infatti, sono stati modificati 53 articoli su 92 originari, e sono stati introdotti altri 9 articoli. Il decreto legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 221, inoltre, aggiorna il CAD all'ultimo orizzonte tecnologico introducendo i concetti di domicilio digitale, cloud computing e revisione dei CED.
La penultima modifica del CAD è stata introdotta dalla legge 23 dicembre 2014, n. 190. L'ultima modifica del CAD (cd. "CAD 3.0") è stata introdotta dal decreto legislativo. n.179 del 2016. La modifica rientra nel quadro normativo della legge delega n. 124/2015, di riforma della PA (c.d. Legge Madia).

ne di disastro e poter attivare le conseguenti procedure di intervento.
In particolare, devono essere identificate le criticità dei dati delle applicazioni che potrebbero andare perse in un disastro, valutandone l'impatto a livello economico e di immagine. Andrà inoltre valutato se si tratta di informazioni, applicazioni o dati che possono essere facilmente recuperate o meno, e l'impatto che questa criticità di mancato recupero potrebbe causare all'organizzazione.

Il *Disaster Recovery Plan* dovrà identificare obiettivi misurabili per il ripristino del servizio, definire come prepararsi al *Disaster Recovery* e come gestire l'operatività di ripristino vera e propria. In sostanza, nel *Disaster Recovery Plan*, dovranno essere pianificate le contromisure tecnologiche ed organizzative per prevenire e gestire un'emergenza, come ad esempio i sistemi di back-up, firewall, sistemi di accesso attraverso credenziali, profilazione canalizzata degli utenti precludendo certe cartelle o certi dati e agevolando la visione di altri dati, anche a seconda delle mansioni svolte. Saranno altresì identificate le risorse umane necessarie a prevenire o mitigare l'impatto di un disastro, le persone coinvolte, i documenti necessari, le informazioni, le attrezzature e le tempistiche.

Anche il *Disaster Recovery Plan*, così come il *Business Continuity Plan*, è un documento che una volta prodotto non può essere statico, ma deve essere dinamico, quindi aggiornato e ammodernato a seconda delle esigenze, delle nuove tecnologie disponibili e delle nuove realtà che si vengono a creare in un'azienda o in un'organizzazione.

Il *Disaster Recovery Plan* si fonda infatti sul principio del miglioramento continuo e ispirato dal buon senso; una volta redatto deve essere testato per verificarne l'efficacia con tutte le unità coinvolte, cogliendo l'opportunità di migliorare i punti deboli. In questa fase devono emergere tutte le possibili anomalie che risultano in fase di applicazione delle procedure descritte sul documento, che andranno quindi annotate per poter efficacemente gestire le opportunità di miglioramento.
Identificate ed analizzate le anomalie, si pongono quindi in essere tutte le misure necessarie a far sì che le stesse rientrino, monitorando le soluzioni adottate e valutando l'efficacia delle stesse.
Il *Disaster Recovery Plan* è quindi un documento dinamico, proprio perché nel tempo possono cambiare molte variabili, quali le attrezzature, le infrastrutture informatiche o i sistemi di back-up, nonché le criticità dei dati stessi.

Gli *hacker*, come noto, sono degli esperti di sistemi e sicurezza informatica abili nell'introdursi in reti protette e in generale nell'acquisire un'approfondita conoscenza dei sistemi sui quali intervengono, per poi essere in grado di accedervi o adattarli alle proprie esigenze. Sono "figure" in continua evoluzione, capaci di sviluppare strategie sempre più efficaci per introdursi nei sistemi informatici. Questa *escalation*, di conseguenza, stimola le organizzazioni a stare sempre al passo tecnologico per contrastare gli attacchi informatici.

L'attività del Security Manager si pone quindi in maniera trasversale rispetto ad una pluralità di discipline, anche diverse tra loro, ma che di fatto hanno una "ossatura comune" che è proprio la gestione della qualità, come contemplato nella revisione del 2015 della norma 10459, che impone all'organizzazione di gestire il rischio, anche non soddisfacendo i requisiti richiesti dal cliente. Discipline diverse dai nomi diversi, ma con uno scheletro comune a tutte le attività in capo al Security Manager.

Momento fondamentale dell'attività del Security Manager, nel contesto in esame, è la realizzazione della *Business Impact Analysis* per poter poi realizzare il *Business Continuity Plan*, che può, peraltro, contemplare anche il documento di *Disaster Recovery*.
In fase di *Business Impact Analysis*, quindi, si andranno a gestire, con il contributo dei responsabili, i sistemi di *Information e Communication Technology*, si indentificheranno le applicazioni critiche per l'organizzazione (*Business Criticality*), per il prosieguo delle normali attività operative. Si identificheranno, altresì, le infrastrutture tecnologiche su cui sono installate le applicazioni o su cui risiedono i dati critici per l'organizzazione, comprendendo la vulnerabilità e i punti deboli degli ambienti tecnologici, individuando le aree a maggior rischio ed i tempi di ripristino.

Questo è il processo complessivo di sviluppo del *Disaster Recovery Plan*, cioè le metodologie che permettono di identificare il rischio nelle sue più ampie sfaccettature qualitative e quantitative, l'impatto e le capacità di identificare il rischio, la minaccia, l'impatto sulle attività e quali siano i controlli da mettere in campo, la misura preventiva detettiva volta all'intercettazione e alla correzione dell'anomalia.

È evidente che non tutte le tecnologie che tendono a proteggere un sistema informatico debbano essere padroneggiate dal Security Manager, che deve invece avere un approccio metodologico utile alla definizione del *Disaster Recovery Plan*, cioè all'identificazione rischi, della minaccia, dell'analisi con ponderazione e del trattamento da prendere in considerazione, cioè la stessa metodologia che troviamo nelle altre discipline. È altrettanto utile che il Security Manager padroneggi comunque i concetti fondamentali che gli consentano di interfacciarsi con i professionisti dell'*Information Communication Technology*, che potranno essere interni all'organizzazione oppure consulenti esterni.
Il Security Manager assume quindi il ruolo di capo progetto di un'attività a più ampio respiro, volta a garantire sicurezza agli impianti informatici e tecnologici.

Alcune delle tecniche per salvaguardare il dato sono il salvataggio su particolari dispositivi o la duplicazione su sistemi in continua evoluzione, che possono essere collocati all'interno delle strutture dell'organizzazione come dei dispositivi per back-up, su dischi o su Nas, oppure sistemi di back-up che possono essere in remoto come cloud o web-farm. Altro aspetto importante da tenere in considerazione è che il back-up o il salvataggio dei dati può essere svolto in modo continuo o ad intervalli di tempo programmati.

Non esiste una regola per compiere delle scelte esatte, ma c'è sicuramente una metodologia da seguire, identificando quali siano i dati più critici e le infrastrutture tecnologiche informatiche più vulnerabili, per trovare poi la soluzione congeniale all'organizzazione considerando i costi e l'efficacia. Lo sviluppo del *Disaster Recovery Plan* deve essere svolto quindi con la partecipazione di tutte le figure dell'organizzazione per capire le varie vulnerabilità, le informazioni critiche per ciascun ambito di competenza e per comprendere in modo sicuro ed efficace come continuare a fare funzionare quel determinato processo.

3. Il Security Manager nelle aziende di sicurezza privata

Come abbiamo visto, un ruolo fondamentale all'interno di un'impresa è rappresentato dal **Security Manager**, cioè da quel professionista in possesso delle conoscenze, abilità e competenze nel campo della security tali da garantire la gestione complessiva del processo di security o di rilevanti sotto processi.

Il Security Manager è, quindi, quel professionista che, all'interno di un'organizzazione aziendale, ha l'obiettivo di tutelarne il patrimonio (inteso nel senso più ampio del termine) garantendo il funzionamento dei suoi processi produttivi e quindi assicurando il mantenimento della capacità di produrre reddito.

Seppur la norma UNI 10459, più volte citata, nasca nel 1995, si è dovuto aspettare il 2010, con il decreto ministeriale 269, perché la figura del professionista della security "entrasse" in un istituto di vigilanza.
A onor del vero, ben prima del 2010, la norma UNI 10891 già prevedeva che all'interno della struttura organizzativa di un istituto di vigilanza dovesse essere presente almeno una funzione con compiti di responsabilità in possesso del profilo professionale di cui alla norma UNI 10459 (norma UNI 10891:2000, punto 6.2.1), ma data la volontarietà della norma, la stessa non aveva avuto grande diffusione. Del resto, si deve considerare che ancora oggi la sicurezza viene ritenta un costo, arrivando al paradosso di pensare di poter ridurre i costi della sicurezza mantenendo inalterata l'ampiezza del perimetro da proteggere.

L'evento dirompente arriva proprio con il citato DM 269/2010, che rende obbligatorie le norme UNI 10891 e 10459 ai fini della capacità tecnica per la gestione di un istituto di vigilanza. L'Allegato A del decreto in questione prevede infatti, al punto 4.2, che l'istituto debba "*essere in possesso della certificazione di conformità alla norma UNI 10891:2000 "Servizi - istituti di vigilanza privata - requisiti" e successivi aggiornamenti, rilasciata da un organismo di valutazione della conformità accreditato*"; l'Allegato B dello stesso decreto, poi, prevede che "*per gli istituti che operano con livello dimensionale 4 e ambiti territoriali 4 e 5 almeno una figura tra il titolare della licenza, l'institore e il direttore tecnico deve possedere il profilo professionale UNI 10459:1995 "Funzioni e profilo del professionista della security" e successive modifiche e aggiornamenti*".
Il combinato disposto delle due norme citate comporta, di fatto, che ogni istituto di vigilanza debba obbligatoriamente disporre della funzione del professionista della security aziendale e che, nel caso di istituti di particolari dimensioni e diffusione territoriale, tale funzione debba anche essere certificata.

Il successivo decreto del Ministro dell'interno n. 115 del 2014, in materia di certificazione della qualità degli istituti e dei servizi di vigilanza privata, fissa precise regole per la verifica della funzione in parola, al punto che l'organismo nazionale di accreditamento, Accredia, ha sviluppato un apposito schema di accreditamento per gli organismi di certificazione che devono occuparsi di tali verifiche di conformità.

Va rilevato come la norma UNI 10459 parli di "*professionista della security aziendale*", proprio perché è l'azienda che ha un interesse precipuo a salvaguardare il proprio patrimonio. Come patrimonio oggetto di tutela non si intendono, evidentemente, le sole risorse economiche e/o finanziarie di un'azienda, ma tutte quelle competenze e caratteristiche che permettono sia di aumentare in maniera considerevole il valore aziendale, sia di generare e produrre reddito e, principalmente, di salvaguardare gli obiettivi raggiunti.

La norma UNI 10459 riassume e descrive le mansioni che svolge il professionista della security aziendale, indicandole come "*...studio, sviluppo ed attuazione delle strategie, delle politiche e dei piani operativi volti a prevenire, fronteggiare e superare eventi in prevalenza di natura dolosa e/o colposa che possono danneggiare le risorse materiali, immateriali, organizzative e umane di cui l'azienda dispone (...), garantire un'adeguata capacità concorrenziale nel breve, nel medio e nel lungo termine*."

Nello specifico, l'azienda alla quale facciamo riferimento è un istituto di vigilanza, che presenta in quanto tale una peculiarità estremamente significativa: esiste ed opera in virtù di un'autorizzazione di polizia, la licenza prevista dall'art. 134 del Regio Decreto n. 773 del 1931 - Testo Unico delle Leggi di Pubblica Sicurezza.

Si tratta di servizi, come ha avuto modo di rilevare il Consiglio di Stato nel parere 1247/2008, "*…nei quali, alla premessa dell'iniziativa economica e delle conseguenti libertà funzionali, vanno collegate quelle di tutela della sicurezza e dell'ordine pubblico e di derivazione delle relative attività da una attribuzione parzialmente riservata o riservabile alla forza pubblica. Questi servizi riguardano attività che per l'incidenza e la qualità delle prestazioni nonché per l'alto grado di pericolo e di specializzazione operativa erano originariamente riservati alle forza pubblica e sono stati progressivamente affidati o consentiti agli istituti di vigilanza e alle guardie particolari, in virtù di specifiche previsioni normative quali ad esempio l'articolo 5 del decreto legge 18 gennaio 1992, n. 9 convertito da legge 28 febbraio 1992, n. 217 e regolamento di attuazione recato nel decreto ministeriale 29 gennaio 1999, n. 85, l'art. 18 del decreto legge 27 luglio 2005, n. 144 convertito con legge 31 luglio 2005 n. 155. Il fenomeno riconducibile, per certi versi, al più ampio concetto della sussidiarietà, implica con evidenza una situazione ad effetti traslativi o derivativi che dir si voglia rispetto alle attribuzioni statuali*".

Pertanto, in considerazione della delicatezza delle funzioni svolte, la legge prevede che l'attività degli istituti di vigilanza sia sottoposta ad un controllo tale da assicurare sia la piena rispondenza agli interessi pubblici primari (integrità fisica e psichica, sicurezza delle proprietà e dei diritti correlati, possibilità di una pacifica vita di relazione), da qualunque soggetto l'attività venga prestata, sia l'intervento immediato ed efficace per ristabilire le predette condizioni, indispensabili per la convivenza civile. Per tale motivo, gli istituti sono sottoposti ad una serie di prescrizioni di legge e regolamentari che ne condizionano e dirigono la costituzione, l'operato e la possibilità di continuare ad operare.
Di tutto questo il Security Manager deve essere profondamente consapevole, ed è con questo che quotidianamente deve sapersi confrontare.

Con riferimento alle competenze e alle conoscenze del Security Manager, si è accennato precedentemente a competenze giuridico-legali, con riferimento specifico ai crimini informatici e alla tutela delle informazioni, a nozioni sul rischio, sulla protezione aziendale e sulla tutela di marchi e brevetti, alle competenze informatiche ed altro.
Nel caso degli istituti di vigilanza, tuttavia, la prima competenza deve essere in materia di legislazione di pubblica sicurezza, fin dal momento della predisposizione della domanda per ottenere la licenza.
L'Allegato C del DM 269/2010 prevede infatti che la stessa rechi, tra le altre cose, il progetto organizzativo e tecnico-operativo dell'istituto, redatto secondo le seguenti indicazioni:

1. *Il progetto organizzativo e tecnico-operativo è predisposto dal soggetto che richiede la licenza ed è presentato al Prefetto unitamente all'istanza di autorizzazione, di cui costituisce parte integrante.*
2. *Il progetto organizzativo e tecnico-operativo deve illustrare dettagliatamente:*
    - *l'ambito territoriale in cui si intende operare;*
    - *il luogo ove l'imprenditore intende stabilire la sede principale, le eventuali sedi secondarie e la centrale operativa dell'istituto;*
    - *le tecnologie che intende impiegare;*

- *la natura dei servizi che l'istituto intende svolgere;*
- *il numero delle guardie che si ritiene di dover impiegare;*
- *la disponibilità economica-finanziaria per la realizzazione del progetto;*
- *i requisiti dell'impresa e del richiedente la licenza;*

il tutto secondo le indicazioni contenute per ciascuna voce negli Allegati A, B ed E del presente Regolamento.

3. *Nella predisposizione del progetto dovrà inoltre tenersi conto:*
   - *della coerenza dei servizi;*
   - *della sicurezza delle guardie giurate;*
   - *delle prescrizioni di sicurezza pubblica, secondo le direttive tecniche impartite dal Ministero dell'Interno - Dipartimento della Pubblica Sicurezza;*
   - *della raggiungibilità operativa delle guardie giurate ed a tal fine si richiede, obbligatoriamente per i servizi di classe A e B, di cui all'art.2, comma 2, lett. a), una sede operativa principale dove si chiede la licenza ed un punto operativo per ogni area funzionale (operatività) distante oltre 100 km, in linea d'aria, dalla sede principale o da altro punto operativo adeguatamente attrezzato con un centro di comunicazioni come indicato nell'Allegato E, per il supporto logistico e la sicurezza operativa del personale impiegato in servizio.*

È di tutta evidenza come la predisposizione di tale progetto presupponga competenze tecnico-giuridiche specialistiche che possono essere riassunte nella figura del professionista della security, il quale, nel caso specifico, dovrà avere un forte *know-how* nel settore della sicurezza privata.
La conoscenza dell'organizzazione dei servizi, della sicurezza delle guardie giurate, nonché delle prescrizioni di pubblica sicurezza, sono certamente frutto di studio, ma non possono in ogni caso prescindere dall'esperienza diretta, "sul campo".
Coniugare sapientemente lo studio e l'esperienza può essere la chiave del successo del professionista della security aziendale nel settore della sicurezza privata, la cui funzione, se correttamente esercitata, può arrivare ad assumere un'importanza strategica ai fini della solidità e della compattezza aziendale.

L'analisi del rischio globale e la relativa gestione, attraverso l'esame degli scenari, della strategia di gestione e controllo, dell'identificazione e valutazione dello stesso, nonché del rischio di *compliance*, degli strumenti di controllo, dell'*enterprise risk management* e della crisi di *management* (in una parola il *risk management*), precedentemente analizzati, deve quindi essere contestualizzata nell'organizzazione e nell'attività di un moderno istituto di vigilanza.
Nel contesto generale il Security Manager si pone in un'ottica di fornitore rispetto alla domanda di sicurezza, sempre più pressante, rappresentando e assolvendo ad una funzione cruciale con riferimento a temi quali la promozione della cultura della sicurezza e l'attività di formazione, ai quali l'impresa deve far ricorso per fronteggiare la crescita delle minacce ed adottare le utili contromisure.
Nella fase di esercizio della propria attività, il Security Manager realizza quindi quel fondamentale raccordo tra pubblico e privato, necessario oggi per far fronte alle nuove e sempre più incalzanti richieste di sicurezza. La globalizzazione dei mercati, l'internazionalizzazione del business, la continua evoluzione tecnologica sono solo alcuni degli aspetti che hanno determinato la nascita di nuovi rischi, per la società in generale e per le imprese di vigilanza in particolare. Tutto ciò ha portato le aziende ad istituire, all'interno della propria organizzazione, una funzione di security sempre più strutturata rispetto al passato.

I macrosistemi aziendali si configurano oggi con un patrimonio intangibile di informazioni, dati, conoscenze, processi e sistemi, che è pertanto necessario presidiare attentamente con nuove sensibilità e dinamiche operative.
Questi nuovi scenari tecnici, economici e di mercato, che configurano un mondo in crescita esponenziale, condizionato dagli incessanti sviluppi tecnologici e dalla globalizzazione, sempre più interconnesso e interdipendente, influenzano fortemente la professione del Security Manager e richiedono un modo nuovo di presidiare rischi e minacce a 360 gradi.
Ai rischi tradizionali di sicurezza fisica e logica si intrecciano nuove e forti esigenze di sicurezza, privacy e *governance* che modificano il perimetro delle attività della security ed ampliano significativamente le responsabilità del Security Manager.

In questo contesto è quindi necessario che il Security Manager disponga anche di una buona conoscenza del business, e rappresenti una funzione che è parte integrante di tutto il sistema, che opera in modo trasversale nei processi aziendali e che è percepita come funzione di supporto, in particolare in un contesto delicato come un istituto di vigilanza.
La necessità di operare in ambiti sempre più delicati, con personale altamente qualificato, idoneo a gestire non solo potenziali rischi nell'espletamento del servizio ma contestualmente a tutelare l'azienda, rendono la funzione del Security Manager oltremodo complessa. Si pensi, ad esempio, oltre a tutti i servizi di sicurezza complementare (custodia, trasporto e scorta di armi, esplosivi e ogni altro materiale pericoloso; custodia, trasporto e scorta del contante o di altri beni o titoli di valore; vigilanza nei luoghi in cui vi è maneggio di somme rilevanti o di altri titoli o beni di valore; vigilanza armata mobile e interventi su allarmi; vigilanza presso infrastrutture del settore energetico o delle telecomunicazioni, dei prodotti ad alta tecnologia, di quelli a rischio di impatto ambientale), a quelli di sicurezza sussidiaria negli aeroporti, nei porti, nelle stazioni o ai servizi in funzione antipirateria a bordo delle navi.

Il lavoro a cui si appresta il professionista della sicurezza deve quindi essere improntato soprattutto alla prevenzione, mediante la predisposizione di quelle misure atte a porre nella condizione di massima sicurezza possibile sia l'istituto che le guardie particolari giurate che operano concretamente sul territorio.
È evidente, quindi, come in tale ottica il professionista della security non costituisca (unicamente) un centro di costo, ma rappresenti un vero e proprio valore aggiunto, capace di creare un ambiente protetto rispetto ai rischi che incombono sull'intera azienda: è il motore di un nuovo modello culturale necessario per affrontare in modo consapevole i rischi operativi, acquisendo in tal modo il riconoscimento da parte degli *stakeholders*.

In un sistema che funzioni, la security rappresenta senza dubbio una funzione in grado di garantire modalità sicure per fare *business*; pertanto, non è solo un'attività "volta a prevenire, fronteggiare e superare gli eventi che possono verificarsi a seguito di azioni in prevalenza illecite e che espongono le persone e i beni (materiali e immateriali) dell'organizzazione a potenziali effetti lesivi e/o dannosi", ma è anche *business orientend*.

4. Il rapporto pubblico/privato

Il Security Manager, come anticipato, può rappresentare anche il punto di congiunzione tra le esigenze pubbliche e quelle private.
La globalizzazione dei mercati, l'internazionalizzazione del business e la continua evolu-

zione tecnologica, sono solo alcuni degli aspetti che hanno determinato la nascita di nuovi rischi, per la società in generale e per le imprese in particolare, sia nel pubblico che nel privato. Tutto ciò ha portato le aziende ad istituire, all'interno della propria organizzazione, la funzione di security in maniera sempre più strutturata rispetto al passato al fine di prevenire rischi, appunto, nuovi. Tutelare l'azienda, salvaguardare le sue risorse umane, economiche e infrastrutturali, significa quindi contribuire a sviluppare, insieme agli altri soggetti pubblici e privati, la rete di tutela del Sistema Paese.

Ciò premesso, per comprendere l'interazione pubblico/privato, è necessario svolgere una serie di considerazioni. Il Regio Decreto n. 773 del 18 giugno 1931 (c.d. TULPS) ha, in effetti, introdotto i primi elementi di sicurezza sussidiaria[40], intesa in senso lato.
L'art. 133, infatti, stabilisce che "Gli enti pubblici, gli altri enti collettivi e i privati possono destinare guardie particolari alla vigilanza o custodia delle loro proprietà mobiliari od immobiliari. Possono anche, con l'autorizzazione del Prefetto, associarsi per la nomina di tali guardie da destinare alla vigilanza o custodia in comune delle proprietà stesse".
Il successivo art. 134 recita: "Senza licenza del prefetto è vietato ad enti o privati di prestare opere di vigilanza o custodia di proprietà mobiliari od immobiliari e di eseguire investigazioni o ricerche o di raccogliere informazioni per conto di privati".

La legge, dunque, introduce forme private di tutela e di controllo, ma opera una netta distinzione di ruoli e funzioni tra vigilanza pubblica e privata, costituendo la prima un potere "sovraordinato" rispetto alla seconda, in ragione dell'esercizio della potestà autoritativa/coercitiva conferitole dalla legge che, invece, manca nella vigilanza privata.

Con la riforma della sicurezza privata, recata dal D.P.R. n.153 del 2008, invece, si realizza la sinergia tra pubblico e privato, nel senso che la sicurezza privata, a parte ogni discorso sull'efficacia degli interventi di repressione tipici della sicurezza pubblica, tende ad affiancarsi a quest'ultima attraverso forme di auto-controllo e, soprattutto, di prevenzione, possibilmente ed auspicabilmente in sinergia con le forze di polizia operanti sui singoli territori.

Del resto, tra gli obiettivi strategici citata Direttiva del Ministero dell'Interno del 2004, vi era quello di "*dare impulso alla sicurezza sussidiaria, con particolare riferimento alla vigilanza privata, nel più ampio contesto di sicurezza generale, armonizzato e controllato dal Ministero dell'Interno e dalle autorità provinciali di pubblica sicurezza*". E' in quest'ottica che nasce il miglior esempio di partenariato pubblico/privato: il protocollo "*Mille occhi sulla città*".
Sottoscritto nel 2010 dal Dipartimento di Pubblica Sicurezza del Ministero dell'Interno, dall'ANCI e dalle Associazioni rappresentative degli Istituti di Vigilanza privata, è la migliore rappresentazione di come la sicurezza pubblica e quella privata, nell'ambito di una cornice regolamentare predefinita, possano procedere sinergicamente, di pari passo e senza dannose sovrapposizioni nella tutela della sicurezza dei cittadini.

Infatti, nella premessa del suddetto Protocollo si fa espresso riferimento:

- ✓ alla sicurezza dei cittadini, alla cui salvaguardia e tutela, in quanto bene comune, concorre l'azione sinergica delle istituzioni e dei privati;
- ✓ alla necessità di sviluppare un sistema di sicurezza che integri le iniziative pubbli-

[40] In realtà già con la Legge n. 690 del 1907 veniva attribuita ai privati e ai Comuni la facoltà di chiedere l'approvazione della nomina di Guardie particolari Giurate per custodire le loro proprietà.

che e quelle private, all'interno di un sistema improntato ai principi di coordinamento e sussidiarietà;
- ✓ alla necessità di realizzare la massima collaborazione tra le Autorità di Pubblica Sicurezza, le Forze di Polizia dello Stato e gli Istituti di Vigilanza Privata, cui è demandato, in forza dell'art. 256 bis del R.D. 635 del 1940 (Regolamento di esecuzione al TULPS) lo svolgimento di servizi di "sicurezza complementare", nei limiti previsti e sanciti dal TULPS stesso.

I "*Mille occhi sulla città*" - consistendo in un canale privilegiato di segnalazione dei reati integrando le forze dell'ordine nell'assicurare la sicurezza nelle aree urbane a tutti i cittadini - rappresentano un modello di sicurezza "integrata" al cui interno i privati possono offrire il loro contributo di conoscenza e informazione, sviluppando un sistema di sicurezza volto ad integrare le iniziative pubbliche e private in una cornice di complementarietà e sussidiarietà, esaltando l'indispensabile ruolo della municipalità. La security diventa così parte di un sistema integrato che assicura la tutela di tutte le componenti della società civile dai rischi.

In questo contesto, la *partnership* tra pubblico e privato si è trasformata in un sistema aperto di integrazione, collaborazione e interdipendenza, e la security si è presentata come snodo e interfaccia tra l'azienda e le Istituzioni.
La collaborazione e la capacità di interazione diventano, quindi, una delle priorità del Security Manager, che deve diventare il *focal point* per mantenere, tra azienda e Istituzioni, rapporti a livello formale ed informale, ferma restando comunque una chiara separazione di ruoli, poteri, competenze.
Il continuo sviluppo della collaborazione tra pubblico e privato consente inoltre di ridurre le spinte private all'autotutela (recentemente manifestatesi in varie forme), nonché di mitigare le gelosie istituzionali mirate alla salvaguardia delle proprie prerogative.
Infine, la collaborazione tra aziende e Forze dell'Ordine richiede anche una maggiore standardizzazione del monitoraggio, la condivisione di database e un approccio comune ai metodi di prevenzione.

Al fine di ottenere successo, appare evidente la necessità di garantire ai professionisti della sicurezza aziendale una formazione continua, sia per i ruoli specialistici e tecnici, sia per i ruoli manageriali.
La formazione e la sensibilizzazione del personale, nonché la partecipazione alle iniziative di cooperazione organizzate dagli Organismi istituzionali dello Stato, sono attività necessarie all'implementazione del sistema di gestione della sicurezza in azienda. alla luce dei continui cambiamenti in questi ambiti.

Come detto, sino a pochi anni fa la funzione di security era considerata esclusivamente un costo per l'azienda. Abbiamo visto invece come questa affermazione sia sostanzialmente errata, anche nel contesto del rapporto pubblico/privato; al contrario, si può sapientemente gestire questo contesto riducendo i costi, attraverso una migliore utilizzazione delle risorse disponibili, ma anche attraverso il giusto ricorso ai fondi ed ai finanziamenti europei stanziati per la sicurezza.

Stiamo quindi parlando di un progetto in continuo divenire, con ampie prospettive di sviluppo, che possono essere così riassunte: superamento della visione, pur positiva, della sicurezza partecipata, per andare oltre; acquisizione di una maggiore conoscenza dei rischi e degli strumenti di contrasto nell'ambito della cybersecurity e miglioramento dell'efficienza dei C.E.R.T. (Computer Emergency Response Team); incremento delle atti-

vità di *business intelligence*, per supportare le aziende che operano all'estero e garantire la tutela delle loro risorse umane e delle loro strutture ed impianti.

In questo contesto, è palese come la formazione assuma un ruolo fondamentale.
È quindi necessario fissare nuovi standard, in un'ottica internazionale, ed eliminare le asimmetrie normative a livello globale. Lo scenario è mutato ed in continua evoluzione, lo *status quo* è una minaccia, e bisogna guardare sempre avanti, anticipando chi o cosa ci potrà creare un problema.

È d'altra parte innegabile che il percorso di valorizzazione del Security Manager in ottica di partnership pubblico-privato, fino ad oggi, sia stato rallentato dalle seguenti criticità: mancata valorizzazione del contributo del Security Manager e della sua professionalità per la tutela dell'ente; scarsa considerazione dei vantaggi della partnership per il medesimo fine; asimmetria informativa, frutto di un approccio al tema, che potremmo riassumere citando Pio VII, in: "non vogliamo, non dobbiamo, non possiamo".
Non vogliamo perché la Pubblica Amministrazione considera l'informazione un patrimonio prezioso da difendere da incursioni esterne; il settore privato ha timore di confrontarsi con una Pubblica Amministrazione avvertita come distante e titolare del solo ufficio ispettivo.
Non dobbiamo, risposta spesso opposta dal settore pubblico, trincerato dietro un quadro normativo lacunoso che permette di rispondere in maniera evasiva alle richieste del settore privato; mentre gli operatori privati, allo stesso modo, ritengono di non dover condividere il loro set informativo temendo eventuali inefficienze della PA nella gestione delle informazioni, che possono risultare addirittura controproducenti nella gestione del loro business.
Non possiamo, concetto intuitivo giustamente invocato da chi, nell'amministrazione della cosa pubblica, non può fornire informazioni per il rispetto della giusta esigenza di riservatezza a tutela dello svolgimento di indagini di Polizia giudiziaria e per l'assolvimento dei pubblici poteri.

In risposta a questo, la moderna figura del Security Manager, nel rispetto della dottrina della scienza della sicurezza, deve essere in grado di presidiare rischi e minacce a tutto campo in relazione agli scenari sempre in evoluzione in ambito tecnico, informatico, economico, finanziario, ecc., in un contesto sempre più globalizzato ed interconnesso con le realtà più disparate, e di gestire un partenariato pubblico-privato a 360 gradi.

5. Le infrastrutture critiche Europee

La lotta al terrorismo ha portato il Consiglio dell'Unione Europea a emanare una Direttiva, la n. 2008/114/CE, in tema di Infrastrutture Critiche.
Con tale termine s'identificano i sistemi, le risorse e i processi la cui distruzione, interruzione o anche parziale o momentanea indisponibilità, ha l'effetto di indebolire in maniera significativa l'efficienza e il funzionamento normale di un Paese, ma anche la sicurezza e il sistema economico-finanziario e sociale, compresi gli apparati della Pubblica Amministrazione centrale e locale.
In altre parole, le infrastrutture critiche sono quelle che consentono l'erogazione dei servizi che caratterizzano la vita dei paesi occidentali. La loro esistenza e corretta funzionalità è sinonimo di necessità di salvaguardare la qualità della vita.
Caratteristica delle infrastrutture critiche è la loro interdipendenza, che significa che queste ultime non solo sono strettamente interrelate, ma che lo sono anche le misure poste

per la loro protezione. La cooperazione, la comunicazione e la coordinazione non sono quindi solo degli obiettivi da raggiungere a livello nazionale, bensì diventano fondamentali quando si considera il contesto comunitario.
Al fine di incrementare il livello di protezione delle infrastrutture critiche, sia nazionali sia europee, diversi sono gli obblighi cui devono sottostare i Paesi della UE e gli operatori/proprietari delle ECI che ivi sono collocate.
Per ogni infrastruttura, infatti, deve essere formulato un "Piano di Sicurezza per gli Operatori" (Operator Security Plan - PSO). La sopracitata Direttiva fornisce un'indicazione dei contenuti minimi che dovranno essere trattati nel Piano; in particolare, deve identificare i beni dell'infrastruttura critica e le soluzioni in atto o in corso di implementazione per la loro protezione. Scopo del PSO è quello di identificare quegli *asset* che soddisfano i requisiti per essere denominati "Infrastrutture Critiche Europee"; in seguito, occorrerà proporre e implementare soluzioni che ne permettano una capillare ed efficace protezione.

In particolare, il Piano dovrebbe prevedere:

- ✓ un momento di identificazione degli *asset* importanti;
- ✓ una fase di *risk assessment*, durante la quale si devono prendere in considerazione gli scenari riguardanti le minacce più probabili;
- ✓ la progettazione e la messa in atto delle procedure e delle misure di prevenzione e protezione.

Deve inoltre essere nominato un Funzionario di Collegamento in materia di Security (*Security Liaison Officer* - SLO), che avrà il compito di facilitare la cooperazione e la comunicazione con le autorità nazionali competenti in materia di protezione delle infrastrutture critiche, la cui presenza è essenziale, dal momento che, come ribadisce la Linea Guida all'implementazione della Direttiva, costituisce il prerequisito per poter formulare il PSO. Non è specificata la tempistica massima per la nomina del Funzionario; in ogni caso, dovrà essere in carica in tempo per preparare il PSO entro la scadenza dei termini prevista per quest'ultimo.

6. Il Security Manager e il segreto di Stato

Il 16 aprile 2008 sono entrate in vigore, a seguito della pubblicazione in Gazzetta Ufficiale, le nuove norme in materia d'individuazione di informazioni, documenti, atti, attività e luoghi suscettibili di essere oggetto di segreto di Stato.
È quanto contenuto nel Decreto del Presidente del Consiglio dei Ministri 8 aprile 2008 il quale, "*in attuazione dell'art. 39 della legge 3 agosto 2007, n. 124, disciplina i criteri per l'individuazione delle notizie, delle informazioni, dei documenti, degli atti, delle attività, delle cose e dei luoghi suscettibili di essere oggetto di segreto di Stato, nonché individua gli uffici competenti a svolgere, nei luoghi coperti da segreto di Stato, le funzioni di controllo ordinariamente svolte dalle aziende sanitarie locali e dal Corpo nazionale dei vigili del fuoco*".

In particolare, il provvedimento stabilisce che potranno essere oggetto del segreto di Stato le notizie, le informazioni, i documenti, gli atti, le attività, i luoghi e ogni altra cosa la cui diffusione sia idonea ad arrecare un danno grave a interessi supremi da difendere con il segreto di Stato.
Rilevante novità del provvedimento è costituita dalla possibilità, ferma restando la necessità di valutare in concreto ogni singolo caso, di richiedere l'apposizione del segreto

di Stato a notizie, documenti, ecc., attinenti agli impianti civili per la produzione di energia (ad es., siti per il deposito delle scorie nucleari, centrali nucleari, rigassificatori e inceneritori) ed altre infrastrutture critiche.
Il segreto si estende anche agli iter autorizzativi, di monitoraggio, di costruzione e della logistica.

Tra l'altro, art. 261 del Codice penale prevede, per chi rivela un segreto di Stato, una pena non inferiore ai cinque anni di reclusione.

Aldilà di ogni possibile valutazione che coinvolga il merito, il provvedimento rappresenta un utile spunto di riflessione dal punto di vista di una possibile sottoposizione a segreto di Stato d'infrastrutture energetiche qualificate come critiche. Tal eventualità appare più che mai concreta se si riflette sull'importanza che sta assumendo a livello nazionale ed europeo la protezione delle infrastrutture critiche, anche energetiche. D'altra parte, la protezione di alcune di queste infrastrutture ben potrebbe coniugarsi con l'esigenza di tutelare gli interessi dello Stato.
Occorre a questo punto evidenziare come la sottoposizione a segreto di Stato di un'infrastruttura critica di proprietà o detenuta dall'azienda avrebbe evidenti riflessi in tema di security (controllo accessi, rilascio dei NOS, ecc.); e a questo riguardo appare opportuno compiere un successivo sforzo, finalizzato ad una valutazione preventiva sull'implementazione, specie nei siti più critici, di adeguate misure di sicurezza. Se tale valutazione, infatti, si presenta oggi necessaria, la stessa diventa imprescindibile per quelle infrastrutture che, domani, potrebbero essere oggetto di segreto di Stato.

Il primo punto decisivo che connette la legge 124/2007 con le tematiche di security è contenuto nell'allegato del Decreto del Presidente del Consiglio dei Ministri emanato nell'aprile del 2008 - che riporta i criteri per l'individuazione delle notizie, delle informazioni, dei documenti, degli atti, delle attività, delle cose e dei luoghi suscettibili di essere oggetto di segreto di Stato -, secondo cui agli stabilimenti civili di produzione bellica e agli impianti per la produzione di energia e ad altre infrastrutture critiche può essere apposto il segreto.
Il medesimo allegato, al comma 17, specifica che qualunque cosa, luogo, evento, informazione, ecc., coperto dal segreto deve essere dotato di specifiche misure di sicurezza.
Fondamentale anche il Decreto del Presidente del Consiglio dei Ministri del 3 febbraio 2006, recante "Norme unificate per la protezione e la tutela delle informazioni classificate", in cui vengono individuati i compiti del Funzionario alla Sicurezza, mediante il combinato disposto degli artt. 27 e 29.

Con specifico riguardo al Capo VI del predetto DPCM, recante "Tutela delle informazioni classificate nel settore industriale", l'art. 27 sulla "Responsabilità della protezione e della tutela delle informazioni classificate nell'ambito delle imprese", attribuisce tale responsabilità al Rappresentate Legale dell'impresa, prevedendo, in realtà societarie complesse e articolate, la possibilità di delegare tale responsabilità, con l'esercizio dei compiti e delle funzioni in materia di protezione e tutela delle informazioni classificate ad un funzionario, di elevato livello gerarchico ed adeguatamente abilitato ai fini della sicurezza, che assume la denominazione di Funzionario alla Sicurezza.

Il successivo art. 29, "Compiti del Funzionario alla Sicurezza della sede principale od unica dell'impresa", disciplina le attribuzioni e le relative competenze di tale figura, elencando dettagliatamente compiti e responsabilità.

Il combinato disposto di questi due articoli, con esame connesso tra responsabilità dell'impresa nella tutela delle informazioni classificate e compiti attribuiti in materia al Funzionario alla Sicurezza, induce ad affermare che, in realtà societarie complesse, articolate e rilevanti per dimensioni, fatturato, ecc. la necessità di visione di insieme delle attività di tutela poste in essere dalla funzione aziendale della Security e l'esigenza di unitarietà nei rapporti con le istituzioni del comparto, fa ritenere funzionale ed opportuno che l'incarico di Funzionario alla Sicurezza possa essere espletato dal **Security Manager** della Società.
Ecco, quindi, come si chiude il cerchio sulla figura che abbiamo analizzato nel presente lavoro, anche in un contesto estremamente delicato e complesso, quale quello del segreto di Stato.

CONCLUSIONI

La nuova vigilanza privata è un sistema aperto alla concorrenza, che vede il miglioramento della tutela delle guardie giurate, della loro professionalità e delle condizioni di sicurezza in cui esse operano, ma anche il miglioramento della qualità dei servizi erogati al cliente dalle aziende, che per poter operare devono essere in possesso di specifici requisiti di qualità, tra i quali sicuramente quello di disporre di funzioni aziendali coerenti con l'evoluzione normativa e con le esigenze di sicurezza.
Abbiamo quindi esaminato la principale novità nell'ambito della normativa *privacy,* evidenziando come si sia passati da un regime europeo regolato da una Direttiva, caratterizzata da norme elastiche che lasciavano agli Stati membri ampi spazi di manovra, ad un Regolamento che, pur per sua stessa natura più rigido (a causa della necessità di legiferare sulla materia della protezione dei dati personali in modo univoco ed uguale in tutti i Paesi dell'Ue) e di uniforme applicazione in tutti gli Stati membri, si mostra però, in alcuni punti, più flessibile, ed in particolare aperto a spazi di manovra, in capo, questa volta, non al legislatore, ma agli stessi titolari del trattamento. Abbiamo poi sottolineato che la protezione dei dati personali è inevitabilmente connessa all'evoluzione tecnologica che, negli ultimi anni, sta avanzando a dismisura, tanto che risulta sempre più difficile per la società e per il diritto stare al passo con essa. Di conseguenza, prevedere una normativa eccessivamente rigida e dettagliata avrebbe avuto come risultato un prodotto legislativo che nel giro di pochi anni sarebbe divenuto obsoleto, già vecchio prima ancora di essere applicato.
Il Regolamento rappresenta perciò una grande opportunità di sviluppo per ogni tipo di impresa, considerata la trasversalità della materia: le grandi aziende di sicurezza privata italiane (o quelle che aspirano ad esserlo) devono saper cogliere le possibilità fornite dal Regolamento per rimanere competitive, rinnovare i propri principi etici e valorizzare al meglio i propri *asset*.
Sul piano della *security*, poi, abbiamo visto come il legislatore abbia colto tutti gli aspetti fondamentali di questo delicato e complesso universo, frammentandoli in varie iniziative legislative, ma tutte con un minimo comune denominatore: analisi del rischio, prevenzione delle minacce diversificate, piani di security, nomina del funzionario alla sicurezza, necessità di conferire tali attribuzioni di responsabilità a figure competenti, qualificate e dotate della necessaria autorità, rappresentano gli elementi cardine su cui si fonda la moderna security.
Il contesto disegnato dalla normativa, sia cogente che volontaria, di riferimento, pone grande attenzione alla minaccia, anche a quella definita atipica, che deve essere monitorata da una funzione professionale con le necessarie competenze. In questo modo, anche il nostro Paese si allinea con molti altri paesi occidentali che, da diversi anni oramai, hanno preso atto dei cambiamenti in tema di sicurezza a livello globale.
La sfida è quella di far si che il Security Manager diventi l'interlocutore obbligato per conoscenze, competenze, capacità di azione e reazione alle emergenze.
La sicurezza impone - in particolar modo in alcuni campi come, ad esempio, quello delle infrastrutture critiche - un approccio globale che coinvolga il settore privato non solo nella situazione di crisi, ma anche e soprattutto nella definizione dei piani e delle contromisure idonee a prevenire il rischio, sotto qualunque forma questo si manifesti.
Due figure, quindi, il DPO e il Security Manager, che rappresentano perfettamente l'evoluzione della sicurezza privata e che costituiscono un'importante opportunità per le aziende e per i professionisti.

BIBLIOGRAFIA

Garante Privacy, "*Cosa intendiamo per dati personali?*";

Open symbol blog, "*GDPR, cosa comporta per le aziende*";

V. Zeno-Zencovich ,"*Intorno alla decisione del caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*", in Dir. Inf., luglio-ottobre 2015;

Antonio Ciccia Messina e Nicola Bernardi, "*Privacy e regolamento europeo 2016/679*";

Lorenzo Notari , "*il dado è tratto*";

Andrea Reghelin, "*L'accountability nel Regolamento Generale sulla protezione dei dati*";

Alessandro Frillici e Patrizia Ghini, "*GDPR e data breach, ecco le linee guida per l'applicazione*";

Bruno Saetta, "*Privacy by design e by default*";

Working Party 29 per la protezione dei dati, "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*";

Andrea d'Agostino e Gioia Girotto, "*Il Data Protection Impact Assessment "DPIA": cos'è e come svolgerlo*";

EU GDPR Compliant, "*Diritti individuali nel GDPR*";

Andrea Giulia Monteleone, "*Il diritto alla portabilità dei dati. Tra diritti della persona e diritti del mercato*";

Mattia Iurato, "*GDPR: mero adempimento o possibilità di sviluppo?*";

AAVV, "*Movimentazioni merci pericolose*", Milano, INAIL, 2007;

Claudio Pierini, G. Lugoboni, P.R. Pais, "*Antincendio e procedure di emergenza in azienda, Roma 2007*";

Vincenzo Acunzo, "*Collaborazione tra forze dell'ordine e istituti di vigilanza privata- La sicurezza sussidiaria all'epoca della riforma della sicurezza privata*", Roma 2014.

<u>Fonti aperte:</u>

Gnosis, "*Rivista italiana di intelligence*";

Renzo Brolis, "*La sicurezza nei luoghi di lavoro: formazione e prevenzione*", Brescia, La Scuola, 2006;

Renzo Brolis, "*Salute e sicurezza negli ambienti di lavoro*", Firenze, Giunti, 1996;

Umberto Saccone, "*Il ruolo del security manager*", Roma, Rassegna dell'Arma dei Carabinieri, 2010, n. 1-2;

Umberto Saccone, "*La Security aziendale nell'ordinamento italiano*", Roma, Gruppo 24ore, 2010.

Grafica ed impaginazione a cura di Mariarosaria Sardelli

FederSicurezza

Via Lucania, 13 – 00187 Roma
Tel. 06.42014405 – Fax 06.49388119
info@federsicurezza.it

Seguici su:
www.federsicurezza.it