La valutazione del rischio Privacy

Perché valutare il rischio per la protezione dati

Sebbene il Regolamento UE 679/2016 (ormai più noto con l'acronimo inglese, GDPR) indichi diverse volte la necessità di effettuare una valutazione dei rischi che incombono sui dati personali, in molte organizzazioni non c'è una chiara evidenza di un processo documentato di valutazione dei rischi che abbia portato ad intraprendere determinate azioni e misure di sicurezza.

Già all'art. 25 (**Privacy-by-design & privacy-by-default**), comma 1, il GDPR ci indica la necessità di effettuare una valutazione dei rischi:

> Tenendo conto dello **stato dell'arte** e dei **costi** di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei **rischi** aventi **probabilità** e **gravità** diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

E all'art. 32 (**Sicurezza del trattamento**), comma 1, riprende:

> Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative ade-guate per garantire un livello di sicurezza adeguato al

> rischio, che comprendono, tra le altre, se del caso: ….

Ancora all'art.35 (**Valutazione di impatto**), comma 1, viene indicata la necessità di valutare un rischio:

> Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del tratta¬mento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Per non parlare poi della "**Notifica delle violazioni dati**", del trasferimento di dati extra-UE e di tutti i considerando che citano i rischi.

Ma come dare evidenza della valutazione dei rischi? E di quali rischi stiamo parlando?

Il processo di valutazione dei rischi sul trattamento dei dati personali è orientato a valutare – e mitigare, se non ridurre al minimo – tutti **i rischi per i diritti e le libertà dell'interessato** che si possono verificare a fronte di un trattamento di dati personali.

Se poi, a valle di una valutazione dei rischi si ottiene un **rischio elevato** per i diritti e le libertà dell'interessato, allora sarà necessario condurre anche una valutazione di impatto sul trattamento che è risultato di rischio elevato. Questo al netto delle altre condizioni che possono portare a condurre comunque una valutazione di impatto, come imposto dal GDPR stesso e dalle indicazione dei Garanti nazionali.

Per essere coerenti con quanto disposto dal Regolamento occorre valutare i rischi analizzandone **gravità** delle conseguenze e **probabilità** di accadimento, come ci indica l'articolo 32.

Un buon modo per affrontare la valutazione dei rischi è sicuramente costituito dall'opportunità di riferirsi a standard internazionali per la valutazione dei rischi, come le norme della serie ISO 31000 (cfr. UNI ISO 31000:2018 – Gestione del rischio – Principi e linee guida).

Dunque, scartando le valutazioni dei rischi privacy svolte un po' "a sentimento" ed in modo discorsivo e piuttosto sbrigativo, come se ne vedono in diverse organizzazioni, vediamo come condurre una valutazione dei rischi che possa metterci al sicuro da sanzioni. Se non altro per aver seguito un ragionamento coerente, basato su dati di fatto e valutazioni oggettive giustificabili.

Premesso che la valutazione dei rischi (o *risk assessment*) è per lo più una valutazione soggettiva che **non pretende di misurare in maniera oggettiva il livello di rischio assoluto**, ma semplicemente di **stabilire le priorità**, mettere in fila i rischi per stabilire, poi, su quali agire con azioni di mitigazione e quali reputare accettabili.

La metodologia di valutazione del rischio

Nel processo di *risk assessment privacy* vengono considerati i seguenti attributi dei dati personali (o degli archivi, banche dati di dati personali):

- RISERVATEZZA: il dato deve essere accessibile solo a chi è autorizzato a conoscerlo.
- INTEGRITÀ: i dati devono essere integri, esatti e coerenti.
- DISPONIBILITÀ: i dati devono essere sempre disponibili alle persone autorizzate quando necessario.

Pertanto, tutti i rischi che possono derivare da trattamenti non conformi ai requisiti normativi sulla protezione dei dati personali possono essere indirizzati ad una o più dei suddetti attributi delle informazioni personali gestite.

In ambito privacy sono considerati solo i rischi relativi al trattamento dei dati personali che hanno impatto sugli interessati (danni materiali ed immateriali). Sono escluse dal contesto tutte le conseguenze di rischi che non hanno impatti sui dati personali.

Le sorgenti di rischio nell'ambito del trattamento di dati personali possono riguardare:

- personale interno all'organizzazione: dipendenti, collaboratori, ecc.
- persone esterne all'organizzazione: fornitori, concorrenti, terze parti, ecc.
- risorse tecnologiche: virus informatici, malfunzionamenti e crash di sistemi, ecc.
- eventi naturali e non naturali (causati dall'uomo): terremoti, incendi, alluvioni, ecc..

Il processo di valutazione dei rischi comprende le seguenti fasi, descritte nel seguito del presente documento:

1. Identificazione dei rischi
2. Analisi e ponderazione dei rischi
3. Identificazione e valutazione delle opzioni per il trattamento dei rischi
4. Attuazione di controlli per il trattamento dei rischi
5. Accettazione/Trattamento dei rischi residui.

Il regolamento ci invita a valutare il rischio con l'ormai nota formula **R= f(G, P)**

dove spesso la funzione è semplicemente una moltiplicazione dei parametri Gravità e Probabilità, misurati attraverso una scala quali-quantitativa (1, 2, 3,… valori che corrispondono a valutazioni del tipo Basso, Medio, Alto…). Tuttavia, restano ancora molti dubbi su come approcciare la valutazione dei rischi per essere ragionevolmente tranquilli della conformità del processo.

Al di là della teoria molto estesa disponibile sull'argomento (le metodologie di *risk assessment* sono molto diffuse in diversi settori ed ambiti), sono stati pubblicati dei modelli pratici per valutare il rischio privacy. Si va dal Modello VERA (*Very easy risk assessment*) ideato da @Cesare Gallotti per la gestione del rischio ISO 27001 (sicurezza delle informazioni) da cui è stato mutuato un "modello VERA Privacy", al modello di risk assessment dell'ENISA, poi modificato da @Stefano Posti e @Cristina Cecere (Metodologia Smart).

Proviamo ad esaminare quanto di buono hanno questi modelli e quanto possono essere applicabili nelle organizzazioni anche di medio-piccole dimensioni che però trattano dati personali abbastanza critici.

Quali sono i rischi privacy?

Tenuto conto che il Regolamento UE indica di tenere in considerazione i rischi derivanti da:

- *Distruzione*
- *Perdita*
- *Modifica*
- *Rivelazione o divulgazione*
- *Accesso non autorizzato*

in modo illegale o accidentale, a dati personali trasmessi, conservati o comunque elaborati. Possiamo fermarci a queste macro categorie di rischio? In alcune situazioni la risposta può essere affermativa, ma va inquadrato con l'approccio giusto tutto il processo di valutazione del rischio.

Occorre pertanto partire dai trattamenti di dati personali, ovvero dal **registro dei trattamenti**, la cui definizione è un prerequisito per la definizione di una valutazione dei rischi privacy.

Alcuni modelli di *risk assessment privacy* partono dai trattamenti e, per ogni trattamento, elaborano una valutazione del rischio in funzione di minacce, vulnerabilità, probabilità di verificarsi delle minacce e relativo impatto/conseguenza.

Il modello ENISA (e la sua revisione Smart di @Stefano Posti) partono proprio dai trattamenti, formulando un esempio relativo al trattamento dei dati del personale dipendente, comune a tutte le organizzazioni.

Prima di illustrare la metodologia è bene evidenziarne subito le criticità: partendo dai trattamenti dovremo elaborare una valutazione dei rischi – piuttosto articolata – per ogni singolo trattamento; ovvero l'analisi dovrà essere ripetuta con i medesimi step per tutti i trattamenti. Va da sé che se i trattamenti individuati sono molteplici, l'analisi dei rischi diventa un esercizio piuttosto dispendioso di energie. Da un lato bisognerebbe avere un Registro con pochi trattamenti, ovvero raggruppare singole attività di trattamento in processi di trattamento più generali (ad es. la "gestione del personale" deve costituire un unico trattamento senza scomporlo in tante attività che lo compongono: elaborazione buste paga, organizzazione del personale, gestione formazione del personale, assunzione nuovo personale, ecc.), dall'altro si rischia di replicare le stesse considerazioni ed analisi su rischi di origine ICT che incombono su tutti i trattamenti o quasi. Questo perché le minacce che provengono dagli strumenti informatici (virus, attacchi hacker, violazione di dati…dovuti a vulnerabilità della gestione dei dati digitali) probabilmente sono le medesime per diversi trattamenti che prevedono la gestione attraverso la stessa infrastruttura IT, gli stessi software gestionali.

Altra carenza del modello ENISA sopra citato è il seguente: lo schema per la valutazione del rischio ENISA vale principalmente per i rischi in materia di sicurezza dei dati, ma il GDPR fa riferimento, in modo più generale, ai "rischi per i diritti e le libertà delle persone fisiche". Dunque – come evidenziato nel "Manuale del RPD" del progetto T4DATA – ci potrebbero essere rischi per i diritti e le libertà dell'interessato che non sono legati alla sicurezza del dato, ovvero alla sua perdita di riservatezza/integrità/disponibilità, bensì sono insiti in un trattamento particolarmente a rischio.

Tale trattamento potrebbe essere uno di quelli compresi fra quelli per i quali è necessaria una valutazione di impatto (DPIA) che, seppur svolto seguendo buone prassi di protezione dei dati, per sua natura, potrebbe comportare ugualmente rischi per i diritti e le libertà dell'interessato. Tra essi vi sono, ad es. la sorveglianza sistematica di zone accessibili al pubblico, il trattamento su larga scala di dati particolari, specialmente se si utilizzano nuove tecnologie (app mobili, sistemi di geolocalizzazione, ecc.), profilazione, ecc.

Dunque, abbiamo dei rischi legati alla sicurezza del trattamento e rischi legati alla valutazione di impatto sui diritti e le libertà dell'interessato. Nello specifico quali potrebbero essere questi rischi? Alcuni esempi possono essere dedotti dalle varie Linee Guida sulla Valutazione d'impatto:

- Discriminazione
- Furto d'identità
- Decisioni ingiuste derivanti da profilazione
- Mancata concessione di un credito
- Limitazione all'esercizio della libertà di espressione
- Spamming
- Telefonate indesiderate

Per tutti i trattamenti che ricadono sotto la valutazione di impatto secondo l'art. 35 del GDPR occorre comunque effettuare una valutazione di impatto.

Altri rischi, non necessariamente legati alla sicurezza dei dati, possono incombere sui diritti e le libertà dell'interessato e, di conseguenza, costituire un *rischio di compliance privacy* per il titolare/responsabile del trattamento. Tra essi ricadono:

- L'impossibilità – per l'interessato – di esercitare i propri diritti di accesso, modifica e cancellazione dei dati personali
- Il trasferimento dati personali fuori UE senza adeguate garanzie
- La raccolta di dati eccedente le finalità
- La conservazione di dati per un tempo eccessivo
- Le informative e consensi incomplete, inesatte o comunque inadeguate

Tutte situazioni che possono comportare reclami dell'interessato oppure istanze al GPDP con eventuale richiesta di risarcimento danni.

Nella determinazione dei rischi privacy ci si potrebbe fermare ad alto livello, identificando i fattori di rischio suggeriti dal Regolamento UE 679 all'art. 32 (vedi sopra: Distruzione, Perdita, Modifica, Divulgazione…) oppure individuare **l'effetto finale per la persona fisica** provocato dall'evento avverso: discriminazione, ricatti, danni morali, furto d'identità, impossibilità di accedere ad un servizio per indisponibilità dei dati,…

Il primo approccio è, tutto sommato, quello adottato dal modello VERA privacy precedentemente citato, anche se i suddetti fattori di rischio sono "incrociati" con una serie di minacce che incombono sui dati, sia in formato digitale, sia su supporto cartaceo.

Un approccio intermedio potrebbe essere basato sulla determinazione di 10-15 rischi "classici" che derivano da un'analisi delle minacce e delle vulnerabilità possibili, calcolando il valore del livello di rischio per ogni rischio, indipendentemente dai trattamenti sui quali impatta o, meglio, considerando globalmente tutti i trattamenti che possono essere affetti dal rischio, considerando il caso peggiore.

La valutazione del rischio secondo i modelli ENISA e SMART

Il modello ENISA, rielaborato nel modello Smart, prevede la valutazione del rischio secondo il medesimo schema, che andremo a descrivere, per ogni trattamento individuato nel Registro dei trattamenti.

Per prima cosa al trattamento vengono assegnati dei **livelli di criticità**

dell'impatto (da 1 a 4) relativi ai consueti attributi di Riservatezza, Integrità e Disponibilità. Tale valutazione viene poi giustificata con note esplicative, caratterizzazione delle tipologie di dati trattati, tempo massimo di indisponibilità dei dati ritenuto ammissibile e così via.

Vi sono analogie col modello di *risk assessment* proposto dalla Linea Guida ISO 27005 per la sicurezza delle informazioni, dove, però, la criticità delle informazioni viene valutata sugli asset (asset fisico o information asset, tradotto con il termine "bene" in italiano); sommando i valori di R + I + D (da 1 a 3) si ottiene un valore dell'asset dal punto di vista dell'impatto sulle informazioni gestite.

Nel modello di rischio presentato, invece, si prende il "caso peggiore" – ovvero il valore più alto fra R, I e D – come valore dell'impatto sul trattamento di dati personali considerato.

I livelli di impatto (gravità) sugli attributi di Riservatezza, Integrità e Disponibilità sono determinati secondo i criteri esposti nella seguente tabella

Livello di impatto	Descrizione
1 = Basso	Piccoli inconvenienti superabili senza particolari problemi (tempo necessario per re-inserire informazioni, irritazione, ecc.)
2 = Medio	Inconvenienti significativi, superabili con alcune difficoltà (costi aggiuntivi, mancato accesso a servizi aziendali, timori, difficoltà di comprensione, stress, piccoli disturbi fisici, ecc.)
3 = Alto	Conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà (sottrazione di liquidità, inserimento in elenchi negativi da parte di istituti finanziari, danni a beni materiali, perdita dell'impiego, ordinanze o ingiunzioni giudiziarie, compromissione dello stato di salute, ecc.)
4 = Molto alto	Conseguenze significative o irreversibili, non superabili (perdita capacità lavorativa, disturbi psicologici o fisici cronici, decesso, ecc.)

Criteri di definizione della gravità dell'impatto

A questo punto il modello in esame prevede un **questionario** per la determinazione della Verosimiglianza (probabilità) che uno o più eventi avversi si verifichino.

Le domandesono suddivise in **quattro aree principali di valutazione** in termini di **sicurezza dei dati**, ossia:

1. Risorse di rete e tecnologiche (hardware e software)
2. Processi/procedure connessi al trattamento
3. Soggetti e persone coinvolti nel trattamento
4. Settore di attività e scala del trattamento

Per ciascuna area di valutazione, vengono poste cinque domande la cui risposta può essere “Si”, “No” oppure “Non so”. In base alle risposte date l’algoritmo che sta alla base del calcolo (si veda il Manuale ENISA, il Manuale degli RPD e il Modello SMART di @Stefano Posti per i dettagli). In realtà il modello ENISA non illustra un metodo matematico di calcolo della probabilità per ogni area, ma definisce una probabilità – per ognuna delle quattro aree sopra identificate – suddivisa come segue:

- Basso: è improbabile che la minaccia si materializzi.
- Medio: c’è una ragionevole possibilità che la minaccia si materializzi.
- Alto: la minaccia potrebbe materializzarsi

La probabilità finale delle minacce viene calcolata sommando i valori della probabilità per ogni singola area, riconducendo il totale ai medesimi 3 livelli.

Invece il modello presentato nel Manuale del DPO presenta un metodo deterministico dei suddetti valori, per ogni area, in base al numero di risposte affermative alle domande poste per ogni categoria.

Il modello di @Stefano Posti parrebbe più dettagliato, sebbene a fronte delle risposte “Non so” non si determini una probabilità maggiore che si concretizzi una minaccia rispetto alla risposta “Si”. Comunque, il file Excel reso disponibile è modificabile e personalizzabile quindi, a fronte delle risposte dubitative, si potrebbe (e dovrebbe) approfondire l’argomento in quanto esiste una maggiore aleatorietà della valutazione.

Il modello SMART, inoltre, permette di correggere il valore della Verosimiglianza determinato dall’algoritmo, nel caso si ritenga non rispecchi fedelmente quanto presente nella realtà.

Il punteggio così ricavato (i valori vengono ricondotti alla scala 1 = Basso, 2 = Medio, 3 = Alto) può essere associato al punteggio relativo all’impatto delle conseguenze, precedentemente calcolato, per arrivare a un **punteggio complessivo per il calcolo del rischio.**

Il modello SMART prevede il calcolo di un livello di rischio per ognuna delle quattro categorie sopra stabilite (Risorse di rete e tecnologiche, Processi/procedure connessi al trattamento, Soggetti e persone coinvolti nel

trattamento, Settore di attività e scala del trattamento) secondo la formula **Rischio = Max (Verosimiglianza x Max (Impatto), per ogni categoria)**, dunque si considera ancora il c.d. "*worst case*" (caso peggiore).

Il punteggio calcolato viene poi associato ad una descrizione secondo la seguente tabella (il valore del rischio può variare fra 1 e 12):

Livello di rischio
Basso < 3
3 < Medio < 6
5 < Alto < 9
Molto Alto > 8

Questa tabella differisce dal criterio proposto dal metodo ENISA (riportato anche nel Manuale dell'RPD) che prevede la seguente matrice di rischio:

Matrice di rischio modello ENISA

Si noti che il rischio Basso (in verde) è asimmetrico, nel senso che se il punteggio 2 viene ottenuto da un Impatto Basso (=1) e una Probabilità Media (=2) il Rischio sarà giudicato Basso, viceversa se il medesimo valore sarà ottenuto da un Impatto Medio (=2) e da una Probabilità Bassa (=1), il Rischio sarà Medio (colore giallo).

Sia il modello ENISA che il modello SMART prevedono, successivamente al calcolo del rischio sul trattamento, la **definizione dei controlli di sicurezza** (alias "misure di sicurezza tecniche ed organizzative") necessari per mitigare il rischio.

A questo punto è necessario aprire una parentesi sulla metodologia di *risk assessment* adottata.

Il rischio che è stato calcolato è un rischio potenziale o **rischio inerente** che incombe sul trattamento a prescindere dalle misure di sicurezza (controlli) implementati. Infatti, se andiamo ad esaminare le domande del questionario per la determinazione della verosimiglianza (o probabilità) delle minacce viene chiesto, ad esempio, se si svolgono operazioni di trattamento tramite internet e se i sistemi IT sono interconnessi con altri sistemi interni o esterni all'organizzazione, non se si dispone di antivirus aggiornati, firewall, sistemi di controllo degli accessi con password complesse e così via. Dunque, la probabilità che una minaccia si

concretizzi è valutata in termini assoluti, senza considerare le misure di prevenzione e protezione adottate.

Facendo una valutazione sulle misure di protezione, anziché di prevenzione come nel caso degli antivirus, andiamo a calcolare la probabilità che si verifichi un terremoto di magnitudo elevata (è diversa la probabilità se siamo in Sardegna o in Abruzzo), ma non consideriamo se l'edificio aziendale è di recente costruzione ed antisismico oppure no.

Quindi il rischio intrinseco lo dobbiamo mitigare con le misure di sicurezza (i controlli) di cui disponiamo, al fine di ottenere il c.d. **rischio residuo**. Se il rischio residuo sarà reputato troppo elevato, o comunque non accettabile per il profilo di rischio del titolare del trattamento, allora dovremo implementare ulteriori misure di sicurezza.

Dunque, il modello SMART ed il modello ENISA, da cui discende, prevedono la determinazione delle misure di sicurezza, in funzione del livello di rischio intrinseco calcolato precedentemente.

Il foglio Excel del modello SMART riporta tutti i punti di controllo della ISO 27001, raggruppati per un totale di 20 elementi, e per ognuno di essi ne viene data una valutazione a 4 livelli (1- Inadeguato, 2- Parzialmente adeguato, 3- Quasi adeguato, 4- Adeguato, oppure Non Applicabile). Viene quindi calcolato un livello di efficacia dei controlli medio (da 1 a 4) e un livello di vulnerabilità media (calcolato come l'inverso dell'efficacia delle misure di sicurezza, ovvero 5 – valore medio dei controlli). Infatti, il concetto è il seguente: quanto più sono efficaci i controlli di sicurezza (le misure di sicurezza), quanto meno i miei dati sono vulnerabili a fronte del concretizzarsi di una minaccia.

A questo punto viene calcolato il rischio ponderato (ovvero il rischio residuo) come il prodotto del rischio inerente calcolato precedentemente per la vulnerabilità media diviso 4 (per normalizzare il nuovo livello di rischio alla scala definita in precedenza. Così il livello di rischio potrà essere attenuato e riportarsi ad un livello Basso, Medio, Alto o Molto alto in base al quale dovranno essere prese delle decisioni sul trattamento, ovvero stabilire:

- Azioni volte ad **evitare** il rischio, azzerando la possibilità che esso si concretizzi;
- Azioni volte a **proteggere** i dati dalle conseguenze del rischio;
- Azioni finalizzate a **ridurre** la probabilità che il rischio si concretizzi, attraverso l'intensificazione dei controlli preventivi;
- Azioni di **trasferimento** del rischio a terzi (fornitori, assicurazioni,…);
- **Accettazione** del rischio, in quanto non è stato ritenuto opportuno intervenire in base al rapporto costi/benefici delle eventuali azioni di trattamento esaminate.

Se a fronte di azioni di mitigazione non si riesce ancora a ridurre un livello di rischio elevato occorrerà procedere con la Valutazione di Impatto (DPIA) ed eventualmente con la consultazione del Garante per la Protezione dei Dati Personali **prima** di avviare il trattamento.

Il modello ENISA, a differenza del modello SMART, prevede una serie di misure di sicurezza (controlli) mutuate anch'esse dai controlli della ISO 27001/27002, ma **prevede necessariamente l'applicazione di alcune misure** (minime) per i trattamenti con livello di rischio Basso, altre misure previste per i trattamenti con livello di rischio Medio e ulteriori misure tassativamente richieste per i trattamenti con livello di rischio Alto. In pratica la scelta delle misure di sicurezza ritenute adeguate è determinata automaticamente in base al rischio calcolato.

In conclusione, i pregi e difetti di questi metodi:

Pro:

- Riferimenti a normative e linee guida che permettono di dimostrare l'accountability del Titolare;
- Metodologia che recepisce quanto richiesto dal Regolamento in merito alla valutazione della Gravità dell'impatto e della Probabilità del rischio;
- Metodo analitico di calcolo del rischio completo, volendo personalizzabile (file Excel reso disponibile da @Stefano Posti);
- Definizione delle aree/categorie di minacce che permette di esaminare tutti gli aspetti del trattamento;
- Flessibilità nel calcolo del rischio residuo sulla base dei controlli applicati (solo metodo SMART) e nella possibilità di ripetere la valutazione dei controlli a seguito dell'implementazione di ulteriori misure di sicurezza;
- Evidenza dell'effetto di mitigazione dei controlli sul rischio inerente (solo metodo SMART).

Contro:

- Necessità di ripetere la valutazione per ogni trattamento, ma la parte relativa al questionario di *assessment* della verosimiglianza (calcolo della probabilità) e quella relativa ai controlli è duplicabile se applicabile a più trattamenti
- Definizione poco dettagliata delle minacce e della relativa probabilità di accadimento
- Definizione troppo deterministica delle misure di sicurezza da adottare per ogni livello di rischio, peraltro piuttosto severe per una PMI (solo modello ENISA)
- Determinazione del rischio in base ad una matrice di rischio asimmetrica (solo modello ENISA).

Il Metodo VERA

Il primo passo, supportato dal relativo foglio Excel, prevede la valutazione delle minacce (ne sono state individuate 42) in termini di probabilità di accadimento (da 1 a 5) e di attributo R I D su cui impattano.

Per ogni minaccia viene anche determinato se sussiste un rischio privacy afferente alle categorie: distruzione accidentale, distruzione illegale, perdita, modifica, divulgazione non autorizzata, accesso non autorizzato ai dati personali.

Parallelamente viene data una valutazione di adeguatezza per tutti i 114 controlli ISO 27001/27002 (in una scala da 1 a 4, stessi criteri del modello SMART). Conseguentemente il valore della vulnerabilità viene definito come pari a 5 – valore di adeguatezza del controllo (come nel caso precedente).

La vulnerabilità di ogni controllo viene moltiplicata per il **valore base di ogni rischio** per ogni minaccia. Quest'ultimo è calcolato come il valore massimo dell'impatto dei valori R I D (applicabili alla minaccia) per la relativa probabilità di accadimento della minaccia ovvero

Base di rischio = verosimiglianza minaccia x valore dato personale (il parametro RID con impatti sulla minaccia e valore più alto)

Quindi:

Rischio (per ogni minaccia e controllo) = Base di rischio x vulnerabilità

("inverso" del valore del controllo)

Si consideri che non tutte le celle all'incrocio fra controlli e minacce sono valorizzate, in quanto alcune sono ritenute non applicabili a determinati controlli.

Nel foglio specifico "Rischio Privacy", per ogni minaccia viene prelevato solo il valore massimo per tutti I controlli (*worst case*). Dunque, volendo mitigare il rischio bisogna agire o sulla verosimiglianza (probabilità) della minaccia oppure sul controllo meno efficace (vulnerabilità maggiore).

Il tutto, naturalmente, va adeguatamente commentato e giustificato.

Questo metodo da un lato prevede una valutazione molto dettagliata sui controlli (sono esplicitati tutti i 114 controlli della ISO 27001), mentre la valutazione sui dati personali è fatta in modo globale, ovvero viene definito un valore per i parametri R/I/D valido per tutti i dati personali. Sicuramente se dovessero emergere rischi elevati, bisognerebbe scomporre la valutazione per diverse tipologie di dati personali trattati (es. dati del personale dipendente, dati dei clienti, dati dei fornitori e così via).

Dunque, è un metodo “controlli oriented”, non pienamente allineato alla metodologia suggerita (o solo intuita) dal GDPR, che prevede di partire dai trattamenti di dati personali e calcolare i rischi conseguenti. Valgono le stesse considerazioni evidenziate per il metodo ENISA ed il metodo SMART riguardo al focus sulla protezione dei dati e non su tutti i rischi per i diritti e le libertà dell’interessato.

Infine, per applicare questo modello occorre una buona conoscenza della norma ISO 27001 e della linea guida ISO 27002 sui controlli di sicurezza per poter valutare in modo ragionevolmente corretto tutti questi controlli.

Un approccio semplificato “risk oriented” alla valutazione del rischio

I rischi che incombono sui dati che sono identificati afferiscono alle seguenti categorie (conseguenze del danno):

1. Perdita di riservatezza di dati personali;
2. Perdita di riservatezza di dati particolari;
3. Perdita di integrità dati particolari;
4. Perdita di integrità dati personali;
5. Indisponibilità temporanea di dati personali;
6. Perdita (distruzione) di dati personali;
7. Non ottemperanza al principio di liceità, correttezza e trasparenza del trattamento;
8. Non ottemperanza al principio di minimizzazione e di limitazione del trattamento dei dati.

Dalle suddette categorie dipendono i **rischi potenziali** seguenti:

1. Accessi non autorizzati a dati personali su supporto durevole da parte di personale interno;
2. Accessi non autorizzati a dati personali su supporto durevole da parte di personale esterno;
3. Accessi non autorizzati dati personali su supporto elettronico da parte di personale interno;
4. Accessi non autorizzati a dati personali su supporto elettronico da parte di personale esterno;
5. Malfunzionamento degli strumenti informatici con alterazione o perdita di dati;
6. Malfunzionamenti degli impianti e dei servizi accessori con indisponibilità o perdita dei dati;
7. Atti di criminalità informatica con rivelazione o perdita di dati;
8. Atti di criminalità comune con rivelazione o perdita di dati;
9. Eventi distruttivi (naturali, artificiali o dolosi) con perdita o indisponibilità temporanea di dati;
10. Raccolta di dati eccedente la finalità del trattamento;
11. Elaborazione di dati eccessiva rispetto alle finalità, consensi ottenuti,

informative, tempi di conservazione e necessità;
12. Impossibilità di garantire l'esercizio dei diritti dell'interessato.

Come si vede i vari rischi raggruppano una serie di eventi (ad es. tra gli eventi distruttivi naturali o artificiali vi sono terremoti, incendi, inondazioni, esplosioni, atti di terrorismo…) e l'accesso non autorizzato ai dati personali viene declinato sia per il formato dei dati (digitale o su supporto cartaceo o durevole per comprendere anche supporti plastici come badge, lastre di esami diagnostici, ecc.), sia per il fatto che l'accesso non consentito sia da parte di soggetti interni all'azienda o esterni, in quanto il livello di riservatezza richiesto può essere differente.

Di conseguenza gli eventi (minacce) che possono far sì che tali rischi si concretizzino sono stati identificati nei seguenti:

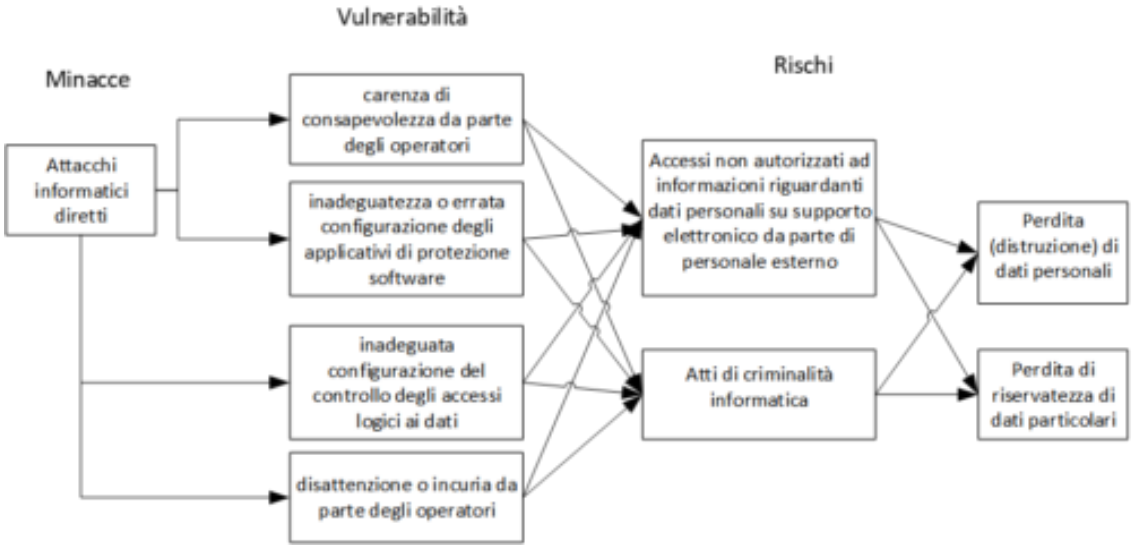
- sottrazione di credenziali di autenticazione da parte di personale interno;
- sottrazione di credenziali di autenticazione da parte di personale interno;
- attacchi informatici diretti da parte di malintenzionati (es. ransomware, phishing);
- furti, rapine ed altri eventi malavitosi;
- comportamenti sleali o fraudolenti di personale interno;
- comportamenti sleali o fraudolenti di personale esterno;
- disastri naturali ed artificiali (alluvioni, inondazioni, terremoti, incendi, ecc.)
- azione di malware non finalizzato;
- intercettazione di informazioni in rete;
- guasto ai sistemi ed impianti complementari (impianto elettrico, climatizzazione, ecc.)
- malfunzionamento dei sistemi informatici gestionali e dei software applicativi;
- inadeguatezza della gestione dei dati personali da parte dei software applicativi e gestionali;
- guasti o malfunzionamenti hardware;
- perdita di dispositivi portatili;

Tali minacce possono concretizzarsi in rischi nel caso in cui incontrino una vulnerabilità nelle misure tecniche ed organizzative di protezione e prevenzione adottate dall'azienda, in particolare:

- carenza di consapevolezza da parte degli operatori;
- disattenzione o incuria da parte degli operatori;
- carenza di conoscenza dei principi del Regolamento UE 679/2016 da parte del personale;
- errore materiale da parte degli operatori;
- inadeguatezza o errata configurazione degli applicativi di protezione software (antimalware, firewall,…);
- inadeguatezza/obsolescenza/malfunzionamento o errata configurazione delle

protezioni hardware (firewall hardware, router, WLAN, IDS,…);
- inadeguata configurazione del controllo degli accessi logici ai dati
- errata gestione (configurazione, utilizzo) dei dispositivi portatili;
- errata gestione del controllo degli accessi all'azienda;
- inefficacia delle misure di sicurezza fisica (controllo accessi, ecc.);
- inefficacia dei sistemi di prevenzione incendi;
- inefficacia dei sistemi di sicurezza fisica (antifurto, porte, armadi chiusi a chiave, ecc.);
- inefficacia dei sistemi di protezione da calamità naturali;
- accessi da parte di esterni non autorizzati (errata applicazione delle regole di accesso fisico al sito);
- insufficiente sorveglianza di strumenti contenenti dati;
- mancata cifratura di dati accessibili a terzi;
- mancata pseudonimizzazione di dati particolari;
- errori umani nella gestione della sicurezza fisica;
- procedure organizzative inadeguate.

A titolo di esempio in Figura sotto sono rappresentati graficamente le minacce, le vulnerabilità ed i rischi legati ad un attacco informatico tipo *ransomware* (es. Cryptolocker, wannacry, ecc.).



In sostanza si fa un'analisi delle minacce e delle vulnerabilità e poi si fa una valutazione dei rischi ponderata sui rischi potenziali indicati nell'elenco numerato sopra riportato.

Partendo dall'approccio basato sull'identificazione dei rischi privacy che incombono sui dati personali sopra esposto si può procedere al calcolo del rischio come segue.

Ad ogni rischio (minaccia) identificato può essere associato un impatto su ogni trattamento di dati personali (ad es. in una scala da 0 a 3), oppure, semplificando ad ogni categoria di interessato di cui sono trattati i dati personali (es. clienti, fornitori, dipendenti, terzi). Evidentemente per ognuna di tali categorie va considerato il caso peggiore, ovvero la categoria di dati personali più sensibile

(dati relativi alla salute, dati economico-finanziari, dati relativi alla religione, piuttosto che dati anagrafici comuni).

A questo punto viene stabilita, sempre per ogni rischio, la **gravità** delle conseguenze nel caso in cui il rischio si concretizzi, in una scala da 1 (impatto trascurabile) a 5 (impatto critico). Naturalmente a fronte ad es. di un accesso non autorizzato a dati personali di un dipendente da parte di personale interno oppure esterno all'organizzazione occorre considerare il caso peggiore di tutti gli effetti possibili (es. furto di identità).

Successivamente, per ogni rischio, va determinata la **probabilità** di accadimento – sempre in una scala da 1 (molto bassa) a 5 (molto alta). Quindi con la classica formula **R = P x G** si ottiene il calcolo del livello di rischio. I valori ottenuti – da 1 a 25 – saranno poi suddivisi in fasce per stabilire, secondo criteri definiti in una matrice di rischio, quali rischi saranno di livello Basso, Medio oppure Alto. Oltre una certa soglia di rischio andranno poi intraprese azioni di trattamento del rischio come indicato in precedenza.

In questo modello, semplificato, prevede che le misure di sicurezza siano ricomprese nella determinazione della Gravità dell'impatto (Misure di Protezione) e della relativa Probabilità (Misure di Prevenzione). In pratica il ragionamento è il seguente: la probabilità di subire un attacco ransomware non viene determinata in modo assoluto (è molto probabile che un attacco ransomware si verifichi), ma in funzione delle misure di sicurezza implementate; per cui si definirà la probabilità che un attacco ransomware abbia successo nonostante le misure di prevenzione attuate (antimalware, sistemi anti ransomware specifici, firewall, formazione del personale per sensibilizzarlo a comportamenti prudenti). La corrispondente gravità sarà determinata considerando le misure di protezione attuate, ad es. la disponibilità di un backup giornaliero cifrato scollegato dal sistema centralizzato.

Volendo mantenere separati gli effetti delle misure di sicurezza dalla probabilità e dalla gravità di un rischio si potrebbe calcolare i valori di probabilità e gravità considerandoli in assoluto, a prescindere dalle misure di prevenzione e protezione adottate, come nei metodi precedentemente illustrati. In tal caso l'effetto di mitigazione delle misure di sicurezza sul rischio potenziale sarebbe definito attraverso un terzo parametro M, che rappresenta l'efficacia delle misure di

sicurezza, espressa in una scala da 1 (Misure molto efficaci) a 5 (Nessuna misura di sicurezza). Il valore per il Livello di Rischio (o indice di rischio) verrà dunque calcolato nel modo seguente:

LR = P x G x M (Probabilità x Gravità x Efficacia delle Misure di Sicurezza)

La scala del rischio sarà conseguentemente da 1 a 125.

In alternativa l'efficacia delle misure di sicurezza potrebbe essere considerata come un fattore di mitigazione del rischio definito dal prodotto P x G, sulla falsariga del modello SMART. Quindi, anziché definire una scala da 1 a 5 per il parametro M, si potrebbe definire una scala di valori del tipo 0.2, 0.4, 0.6….1; ovvero si inverte la scala dell'efficacia delle misure di sicurezza (1 sta per "Nessuna misura", 5 sta per "Misure molto efficaci") e si trasforma la formula precedente nella seguente **LR = P x G / M**.

Conclusioni

Naturalmente possono essere elaborate diverse variazioni sul tema e altri metodi di calcolo del rischio privacy (ad es. mutuandoli dalla metodologia FMEA); il limite è probabilmente solo la fantasia dell'autore del nuovo modello. L'importante è restare legati ad una base normativa standard (ISO 31000 per il processo di valutazione del rischio, Linee Guida ENISA o altre Linee Guida per il calcolo del rischio) e definire una formula corretta per il calcolo del rischio. Alcuni, infatti, anziché moltiplicare i contributi di Gravità, Probabilità e Misure di sicurezza (Controlli) li sommano e ciò non è propriamente corretto.

Diversi applicativi software per la gestione della privacy e dei sistemi per la gestione delle informazioni ISO 27001 hanno implementato un sistema di valutazione dei rischi più o meno articolato e, dunque, possono soddisfare allo scopo.

Riferimenti

1. ENISA – Manuale sulla Sicurezza nel trattamento dei dati personali (dicembre 2017) – § 2 Valutazione del rischio e misure di sicurezza per i dati personali
2. Manuale RPD – Compito 3: Valutazione dei rischi posti dalle attività di trattamento di dati personali
3. VERA 5.0 https://www.cesaregallotti.it/Pubblicazioni.html
4. Metodologia Smart 1.0 https://it.linkedin.com/pulse/strumenti-disponibili-per-la-valutazione-dei-rischi-stefano-posti