# Vademecum Data Breach

Francesco Paolo Micozzi

CIBER Jean Monnet Module

With the support of the Erasmus+ Programme of the European Union

***Il presente vademecum afferisce alle attività del Modulo Jean Monnet "Cybersecurity Issues and Breaches in European Rules: a practical approach" (CIBER) finanziato dalla Commissione Europea, Agenzia EACEA (620505-EPP-1-2020-1-IT-EPPJMO MODULE).***

## SOMMARIO

# Il Vademecum

## 1 Premessa

La digitalizzazione dei servizi delle pubbliche amministrazioni ha portato a innumerevoli vantaggi in termini di efficienza, trasparenza e accessibilità. Tuttavia, la crescente dipendenza dalle tecnologie informatiche comporta inevitabilmente un insieme di rischi associati alla sicurezza delle informazioni. Questo vademecum ha lo scopo di illustrare i principali rischi di sicurezza informatica e fornire delle linee guida su come mitigarli e su come gestire il data breach nei rapporti con l'Autorità. Il vademecum, inoltre, si propone di offrire un quadro delle norme di riferimento in materia.

Il presente vademecum afferisce alle attività del Modulo Jean Monnet "*Cybersecurity Issues and Breaches in European Rules: a practical approach*" (CIBER) finanziato dalla Commissione Europea, Agenzia EACEA (620505-EPP-1-2020-1-IT-EPPJMO MODULE).

## 2 Il rischio

Consideriamo normative come il Regolamento europeo sulla protezione dei dati personali (UE) 2016/679, il D.Lgs. n. 81/2008 sulla sicurezza sul lavoro, la Legge anticorruzione (n. 190/2012) e il D.Lgs. n. 231/2001 relativo alla responsabilità amministrativa degli enti. Queste disposizioni mirano a contrastare e gestire vari rischi, tutti con l'obiettivo comune di proteggere interessi specifici. Nonostante questi rischi abbiano caratteristiche diverse tra loro, l'approccio normativo è costante: è fondamentale non solo identificare misure preventive, ma anche strategie da implementare nel caso in cui tali rischi diventino realtà, al fine di mitigarne l'impatto negativo.

Una caratteristica distintiva che emerge attraverso diverse normative legate alla gestione del rischio (come il GDPR, il D.Lgs. n. 81/2008, la legge n. 190/2012 e il D.Lgs. n. 231/2001) è l'approccio sia

proattivo che reattivo, parallelo a quanto delineato nello standard internazionale ISO 31000 (edizioni 2009 e 2018). Si può osservare che, nei testi normativi menzionati, vi è una chiara ispirazione — spesso manifesta — derivante dai principi e dalle linee guida espresse dalla norma ISO 31000 riguardo alla gestione del rischio.

Lo standard ISO 31000 definisce il rischio in modo semplice ma penetrante come "l'effetto dell'incertezza sugli obiettivi". Questa definizione è abbastanza vasta da includere sia gli esiti potenzialmente dannosi sia quelli vantaggiosi, ossia le opportunità, derivanti dall'incertezza. Pertanto, la norma evita termini come "minaccia" o "pericolo" quando si riferisce alla “fonte del rischio”. Piuttosto, descrive una "fonte del rischio" (risk source) come qualsiasi elemento che, da solo o in combinazione con altri, possa generare rischio. In linea con il risk-based approach o il "risk-based thinking", l'incertezza può aprire le porte non solo a scenari negativi ma anche a potenziali opportunità.

La gestione del rischio porta con sé la stessa incertezza intrinseca al concetto di rischio. Questo sottolinea un punto fondamentale: è quasi impossibile gestire il rischio in modo tale da eliminarlo completamente. Oltre ai rischi noti, che potremmo cercare di prevenire attraverso contromisure specifiche, esistono rischi sconosciuti o imprevedibili, per i quali, data la loro natura imperscrutabile, non potremmo prepararci adeguatamente ad affrontarli da una prospettiva preventiva. Il concetto di "sicurezza", che gli esperti di cybersecurity considerano sempre relativo e mai assoluto, deriva dal latino "sine cura", che significa "senza preoccupazione". Ma questa mancanza di preoccupazione non significa necessariamente “assenza di rischio”, ma dipende dal fatto che alcuni rischi, essendo sconosciuti, sono inevitabilmente imprevedibili.

L'art. 32 del GDPR, ad esempio, non mira a eliminare completamente il rischio. Piuttosto, esige che titolari e responsabili del trattamento assicurino "un livello di sicurezza adeguato al rischio".

Questo suggerisce che, anche se sono state adottate tutte le contromisure possibili, il rischio residuo potrebbe ancora realizzarsi. Tale eventualità, una volta verificatasi, dovrebbe essere considerata come un potenziale rischio nelle future revisioni e aggiornamenti delle strategie di prevenzione.

La gestione del rischio adotta la filosofia del miglioramento continuo, seguendo un approccio iterativo caratterizzato dal noto "ciclo di Deming" di Plan, Do, Check, Act (PDCA), che verrà descritto più avanti.

Secondo la definizione fornita dalla ISO 31000, il rischio è determinato dal prodotto tra la probabilità che un evento avverso si verifichi e la severità del danno che potrebbe causare se dovesse manifestarsi. In termini matematici, il rischio può essere rappresentato dalla seguente formula: $R=P\times G$ (dove R è il Rischio, P è la Probabilità e G è la Gravità). Quest'ultimo fattore, identificato come "G", rappresenta la gravità del danno potenziale. Tuttavia, in alcuni contesti normativi, come nelle disposizioni relative all'anticorruzione, potrebbe essere riferito anche come "impatto". Nonostante la diversa terminologia, il concetto sottostante rimane fondamentalmente lo stesso.

Il concetto espresso dalla formula "R=P*G" è chiaramente rilevante nella normativa europea riguardante la protezione dei dati personali. Questa formula, che lega la probabilità di un evento al suo potenziale impatto o gravità, trova eco in diverse parti del Regolamento Generale sulla Protezione dei Dati (GDPR).

Il GDPR enfatizza ripetutamente l'importanza di valutare i rischi associati al trattamento dei dati personali, in termini sia di probabilità che di potenziale impatto sulle libertà e i diritti delle persone. Come citato, numerosi passaggi del Regolamento fanno riferimento a questa dualità: la probabilità che un determinato rischio si concretizzi e la gravità delle sue potenziali conseguenze.

In particolare, la Valutazione d'Impatto sulla Protezione dei Dati (DPIA) emerge come uno strumento fondamentale nel GDPR. La DPIA è essenzialmente un processo proattivo che aiuta a identificare e valutare i rischi associati a particolari attività di trattamento dati. Se, sulla base di una DPIA, si determina che un'attività di trattamento presenta un alto rischio per i diritti e le libertà delle persone fisiche, e che non sono state adottate misure adeguate per mitigare tale rischio, il titolare del trattamento deve consultare l'autorità di controllo prima di procedere con l'attività.

Quindi, attraverso questi riferimenti nel GDPR, è evidente che la formula "R=P*G" non è solo una mera equazione matematica, ma rappresenta un pilastro fondamentale nell'approccio normativo dell'Unione Europea alla gestione dei rischi associati al trattamento dei dati personali.

## 3 L’acronimo CIA

Nel contesto del trattamento dei dati personali, è essenziale prevenire le violazioni di tali dati. L'art. 4 del GDPR definisce una violazione come un evento in cui la sicurezza è compromessa, portando alla distruzione, perdita, alterazione o divulgazione non autorizzata di dati personali, o all'accesso non autorizzato a tali dati. Questa definizione richiama la triade CIA (Confidentiality, Integrity, Availability): Confidenzialità, Integrità e Disponibilità.

- **Confidenzialità**: I dati sono protetti da accessi non autorizzati
- **Integrità**: I dati non vengono alterati o modificati da soggetti non legittimati
- **Disponibilità**: I dati sono accessibili quando necessario per i soggetti legittimati

Se queste tre condizioni sono soddisfatte, il trattamento dei dati è considerato sicuro secondo l'art. 5 del GDPR. L'art. 32 del GDPR fa riferimento – oltre che alle misure adeguate tecniche ed organizzative che il titolare o il responsabile potrebbero dover adottare «tra le altre

e se del caso» (a significare che l'elenco non è esaustivo e che le misure devono comunque essere valutate caso per caso) – a un altro concetto fondamentale: la "resilienza". Quest'ultima si riferisce alla capacità di un sistema o di un servizio di resistere a un attacco, assorbirne l'urto e tornare alle normali attività nel più breve tempo possibile. Questo articolo suggerisce anche che le misure di sicurezza debbano essere continuamente valutate e aggiornate.

In questo modo si nota che nel GDPR alcune misure specifiche sono finalizzate alla prevenzione (si veda, ad esempio, quanto disposto dall'art. 32 GDPR in cui, in sostanza, tra le misure di prevenzione sono individuate genericamente le misure tecniche ed organizzative adeguate e, nello specifico, la pseudonimizzazione, la cifratura, le procedure di audit delle misure attuate, l'adesione a codici di condotta, nonché quanto previsto in tema di privacy-by-design e privacy-by-default dall'art. 25). Altre misure sono finalizzate ad arginare o limitare gli effetti negativi del rischio una volta verificatosi (si pensi alla misura consistente nella "capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico", di cui all'art. 32, o alle disposizioni relative alla comunicazione e notifica delle violazioni di dati personali, di cui agli artt. 33 e ss., e le relative misure "per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi").

Come già accennato, il GDPR, al pari di altre normative citate come la l. 190/2012, il d.lgs. 81/2008 e il d.lgs. 231/2001, stabilisce non solo i principi da seguire nel trattamento dei dati personali per prevenire rischi ai diritti degli interessati, ma indica anche le azioni da intraprendere quando questi rischi dovessero concretizzarsi.

Nella definizione di "violazione di dati personali" prevista dal GDPR, quindi, ritroviamo tutti gli elementi riconducibili alla triade CIA:

- Disponibilità:

- violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione ai dati personali trasmessi, conservati o comunque trattati.
- violazione di sicurezza che comporta accidentalmente o in modo illecito la perdita dei dati personali trasmessi, conservati o comunque trattati.
- Integrità:
- violazione di sicurezza che comporta accidentalmente o in modo illecito la modifica ai dati personali trasmessi, conservati o comunque trattati.
- Confidenzialità:
- violazione di sicurezza che comporta accidentalmente o in modo illecito la divulgazione non autorizzata dei dati personali trasmessi, conservati o comunque trattati.
- violazione di sicurezza che comporta accidentalmente o in modo illecito l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Nelle discipline normative alle quali abbiamo fatto cenno, la scelta e l'applicazione di misure proattive e reattive non è sempre completamente affidata alla discrezionalità dell'entità destinataria degli obblighi. In certi casi, infatti, il Legislatore stesso specifica quali siano le misure di prevenzione da adottare, riconoscendo implicitamente che tali azioni sono fondamentali ed hanno indubbiamente la capacità di ridurre i rischi. Questo approccio è evidente, ad esempio, nella l. 190/2012, che introduce obblighi di trasparenza, come evidenziato dal "Decreto trasparenza" (d.lgs. 33/2013). Altre norme prescrivono la formazione specifica per i dipendenti sulla prevenzione delle ipotesi di *maladministration* o impongono misure come la rotazione del personale nelle pubbliche amministrazioni.

A differenza di tali normative, il GDPR non elenca misure preventive specifiche come avveniva nel Codice della privacy prima delle modifiche apportate dal d.lgs. 101/2018. Piuttosto, il GDPR affida al titolare o al responsabile del trattamento la responsabilità di

determinare e implementare le "misure tecniche e organizzative adeguate", fornendo una maggiore flessibilità nell'adeguamento alle specifiche esigenze e contesti.

## 4 Le misure di sicurezza

Prima delle sue revisioni per conformarsi al Regolamento Generale sulla Protezione dei Dati (GDPR) attraverso il Decreto Legislativo 101/2018, il Codice della Privacy italiano adottava un approccio piuttosto specifico riguardo alle misure di sicurezza per la protezione dei dati e dei sistemi informativi. In questa normativa era previsto un 'obbligo di sicurezza' generalizzato, all'interno del quale venivano distinte due categorie di misure: quelle 'minime' e quelle 'idonee'.

L'articolo 31, che delineava l'obbligo generalizzato di sicurezza, era volto a minimizzare i rischi legati alla protezione dei dati personali. Questo articolo mirava specificamente a prevenire la distruzione, la perdita accidentale o deliberata, l'accesso non autorizzato e qualsiasi forma di trattamento dei dati non conforme alle norme. Era, in sostanza, un quadro normativo progettato per assicurare che i dati personali fossero trattati in maniera sicura e confidenziale, prevenendo ogni possibile forma di abuso o compromissione.

Questo approccio, con misure specificamente delineate, è stato in seguito rielaborato e reso più flessibile con l'introduzione del GDPR, che, come discusso in precedenza, affida ai titolari e ai responsabili del trattamento una maggiore responsabilità e discrezionalità nella definizione e nell'implementazione delle misure di sicurezza adeguate alle specifiche circostanze e rischi.

Le misure minime di sicurezza - individuate, come abbiamo visto, “nel quadro dei più generali obblighi di sicurezza” - erano definite e catalogate nell’Allegato B (c.d. Disciplinare tecnico) del Codice della privacy. Queste misure si applicavano a tutti i trattamenti di dati personali, indipendentemente dall'uso di strumenti elettronici, come stabilito dagli articoli 34 e 35 del Codice precedente, e la loro mancata

adozione era sanzionata penalmente secondo l'articolo 169, con pene che potevano arrivare all'arresto fino a due anni.

Le cosiddette 'misure idonee', invece, definivano tutte le ulteriori misure di sicurezza che non rientravano in un elenco chiuso. Sia il Codice che il GDPR riconoscono l'impossibilità di eliminare completamente tutti i rischi. Basandosi sulle linee guida ISO 31000 sulla gestione del rischio, entrambi mirano a garantire la confidenzialità, l'integrità e la disponibilità dei dati trattati, lasciando la responsabilità individuale di determinare come raggiungere tale obiettivo.

Con il GDPR si abbandona la tradizionale bipartizione tra misure minime e misure idonee per concentrarsi sulle “misure tecniche e organizzative” adeguate al trattamento. Ed è proprio il titolare (o il responsabile del trattamento) a dover individuare - sulla base di alcuni parametri indicati nell’art. 32 del GDPR - le misure tecniche e organizzative da impiegare caso per caso. Con il principio della accountability (o “responsabilizzazione”), previsto al par. 2 dell’art. 5, infatti, il titolare è (deve essere) oltre che competente a trattare i dati personali “in maniera da garantire un’adeguata sicurezza”, anche in grado di comprovarlo.

Il GDPR stabilisce che le misure di sicurezza devono essere sia "tecniche" che "organizzative". Questo significa che l'art. 32 non si limita agli aspetti puramente tecnici, ma comprende anche le decisioni organizzative. In quest’ambito rientrano, ad esempio, le decisioni circa l’organizzazione interna del titolare, la corretta individuazione dei responsabili del trattamento e del responsabile della protezione dei dati e così via.

L'art. 32 del GDPR stabilisce che sia il titolare che il responsabile del trattamento debbano adottare "misure tecniche e organizzative" proporzionate al livello di rischio associato ai dati personali. Come possono il titolare e il responsabile del trattamento determinare se le misure adottate siano effettivamente proporzionate al rischio? Per

rispondere a questa domanda, occorre fare riferimento ai criteri elencati nell'art. 32 del GDPR:

- Stato dell’arte in tema di misure di sicurezza;
- Costi per l’attuazione delle misure;
- Natura, oggetto, contesto e finalità del trattamento;
- Livello del rischio incombente su diritti e libertà delle persone fisiche.

Il "livello di rischio" a cui fa riferimento il GDPR riguarda qualcosa di futuro, incerto e indefinito che si pone come ostacolo al raggiungimento dell’obiettivo (che in questo caso è la tutela dei diritti e delle libertà delle persone fisiche). Questo rischio può essere valutato considerando due aspetti principali: la probabilità che un particolare rischio si manifesti e l'entità del danno che potrebbe derivarne.

# Situazioni di Rischio e loro prevenzione

## 5 I Rischi di Sicurezza Informatica più Frequenti

Si è già affrontato il tema relativo alla triade della sicurezza: confidenzialità, integrità e riservatezza. Di seguito si illustreranno alcune tipologie di minacce ai sistemi informatici (e di conseguenza ai dati personali e non personali contenuti in essi) tra le più frequenti e in grado di incidere in maniera più o meno significativa su uno o più parametri della triade CIA. È ben possibile, infatti, che la manifestazione di un rischio incombente sulle informazioni possa risolversi, ad esempio, sia in una lesione alla confidenzialità che all'integrità delle informazioni. Questo dipende dalla metodologia di violazione alla quale vadano incontro i dati personali.

## 6 Casi di data breach osservati, di recente, in Europa

Di seguito sono elencati, sia pur in forma succinta, alcuni tra i più recenti provvedimenti sanzionatori adottati dalle Autorità di controllo sulla protezione dei dati personali (le cui funzioni sono descritte nel GDPR) nei confronti dei titolari del trattamento dei dati personali a seguito di data breach.

- Datatilsynet (Danimarca) – caso 2021-431-0163 – Il titolare ha implementato deboli misure di sicurezza sulla propria piattaforma, tanto che gli utenti, accedendo semplicemente agli "strumenti di sviluppo" del browser, riuscivano ad accedere ad informazioni sensibili (errore umano – configurazione)
- IMY (Svezia) – caso DI-2021-3422 – Erroneo invio di email contenenti dati personali (errore umano)
- AEPD (Spagna) – caso E/12707/2022 – Erroneo invio di email ai destinatari sbagliati (errore umano)
- AEPD (Spagna) – caso EXP202303130 – Condivisione dei dati sanitari dei dipendenti senza l'adozione di adeguate misure di sicurezza (errore umano – configurazione)

- AEPD (Spagna) – caso PS/00456/2022 – Verifica dell'identità del soggetto non eseguita in modo sicuro (non è stata confrontata la firma depositata con quella impiegata per accedere al conto corrente) – (debolezza del sistema di autenticazione)
- AEPD (Spagna) – caso PS/00097/2023 – Comunicazione di dati sanitari a soggetti terzi con violazione del principio di finalità (errore umano – erronea applicazione del principio di finalità)
- AEPD (Spagna) – caso PS/00565/2022 – Diffusione di immagini di videosorveglianza che sarebbero state utilizzate in un procedimento disciplinare (errore umano – diffusione illecita)
- NAIH (Ungheria) – caso 6427-1/2023 – Nonostante fosse nota da anni una vulnerabilità del sito web, questa non è stata corretta e ha determinato l'esfiltrazione, da parte di terzi, del database degli utenti (omesso aggiornamento che determina esfiltrazione di dati)
- IMY (Svezia) – caso DI-2021-1905 – Al fine di comunicare dati personali agli interessati veniva impiegato un URL che conteneva una UserID che, modificato nella barra degli indirizzi del browser, consentiva di accedere, senza autenticazione, anche alle informazioni di altri interessati (errore umano – configurazione)
- ANSPDCP (Romania) – decisione del 23.08.2023 – Dipendente pubblica video dell'interessato sui social media e il titolare viene sanzionato (errore umano – omesso controllo – omessa formazione)
- AEPD (Spagna) – caso PS/00388/2022 – Titolare sanzionato perché non ha adottato misure tecniche e organizzative adeguate a verificare l'identità dell'utente prima di concedere, telefonicamente, l'accesso ai dati personali di altro soggetto (errore umano – omessa verifica del legittimato)
- AEPD (Spain) – caso PS/00353/2022 – Comunicazione di dati personali di un dipendente in un gruppo whatsapp (errore umano – comunicazione illecita)
- ICO (Regno Unito) – decisione del 27.4.2023 – Documenti destinati alla distruzione sono stati lasciati incustoditi in un'area accessibile a soggetti terzi che hanno potuto prendere visione del contenuto (errore umano – omesso controllo)
- AP (Olanda) – decisione del 19.1.2023 – Titolare non predispone una procedura di verifica dell'identità. A causa di questo, soggetti terzi

accedono ad informazioni personali (errore umano – omessa verifica del legittimato)

- APD/GBA (Belgio) – caso 17/2023 – Interessato si accorge che qualcuno accede al suo fascicolo due volte e chieste informazioni relative a questo duplice accesso non ottiene risposta. L'autorità di controllo raccomanda di adottare un registro degli accessi al database della PA.
- ANSPDCP (Romania) decisione del 6.3.2023 – Il titolare non predispone idonee misure di prevenzione per attacchi ransomware con esfiltrazione dei dati stessi (attacco informatico – ransomware)
- APD/GBA (Belgio) – caso 16/2023 – Impiegato del settore pubblico si considera titolare di fatto quando tratta dati personali per scopi personali. (in Italia configurerebbe il reato di accesso abusivo a sistema informatico)
- AEPD (Spagna) – caso PS-00480-2022 – Una PA riutilizza il retro di documenti ufficiali come blocco degli appunti (errore umano – omessa formazione)
- Personvernnemnda (Norvegia) – caso 21/00481 – Omessa adozione di misure di sicurezza agevolano attacco ransomware a una PA (errore umano – attacco informatico)
- AEPD (Spagna) – caso PS-00028-2022 – PA pubblica erroneamente un file di excel contenente dati personali (errore umano – diffusione illecita di dati personali)
- GPDP (Italia) – caso 9861289 – Ospedale salva documenti sanitari nella cartella clinica di altro soggetto, consentendo a quest'ultimo di accedere ai dati dell'interessato (errore umano)
- GPDP (Italia) – caso 9863050 – Ospedale comunica via email ad un utente il referto sanitario di un altro utente (errore umano)
- Datatilsynet (Danimarca) – caso 2021-442-12980 – A causa di un errore tecnico in una applicazione che consentiva l'accesso via web a dati personali, i dati personali dell'interessato sono stati accessibili anche a soggetti terzi (errore umano – errore di configurazione)
- ANSPDCP (Romania) – comunicato del 12.1.2023 – Il titolare non implementa adeguate misure di sicurezza per evitare il furto di librerie contenenti dati personali degli impiegati (attacco informatico – perdita di disponibilità e confidenzialità)

- Datatilsynet (Norvegia) – caso 20/02144 – Titolare consente accesso da remoto ai dati degli interessati ma l'unico sistema di autenticazione è il numero di telefono dell'interessato. Questa debolezza consente a chiunque conosca il numero di telefono dell'interessato di accedere alle sue informazioni personali (errore umano – errore di configurazione)
- AEPD (Spagna) – caso EXP202102056 – La PA, anche quando effettua le pubblicazioni per finalità di trasparenza, deve rispettare il principio di minimizzazione del trattamento di dati personali contemplato dal GDPR (errore umano – pubblicazione per finalità di trasparenza)
- ANSPDCP (Romania) – comunicato del 4.1.2023 – Il titolare comunica dati personali (indirizzi email) degli interessati inviando a un gran numero di destinatari una comunicazione email con l'indirizzo email degli interessati nel campo "To" ("a") piuttosto che nel campo "Bcc" ("ccn") – (errore umano)
- Datatilsynet (Danimarca) – caso 2021-442-14071 – Sanzionato titolare per non aver verificato la presenza di errori di architettura nel database contenente dati degli interessati (errore umano – omessa verifica della sicurezza)
- Persónuvernd (Islanda) – caso 2020010355 – Il titolare utilizza un sistema web di gestione della formazione che, a causa delle sue debolezze di programmazione, consente a terzi di accedere alle informazioni degli alunni (errore umano – vulnerabilità)
- AEPD (Spagna) – caso PS/00254/2019 – Con un cyber-attacco tramite SQL injection ai server web del Titolare, gli attaccanti esfiltrano i nomi di coloro che avevano sottoscritto la newsletter. La sanzione viene motivata per non aver predisposto le misure necessarie ad evitare che la SQL injection venisse messa a segno (attacco informatico – esfiltrazione)
- AEPD (Spagna) – caso PS/00342/2022 – Un sindacato dei lavoratori pubblica sui social media i dati personali dei membri del comitato di sciopero, in assenza di una valida base giuridica (errore umano – diffusione illecita)
- NAIH (Ungheria) – caso NAIH-2894-3/2021 – Anche in epoca pandemica, il trasferimento di dati sanitari ai medici non autorizzati,

senza una protezione con password, implica un data breach (errore umano – comunicazione non sicura)

- GPDP (Italia) – caso 9544594 – Titolare contatta l'interessato a un numero di telefono diverso da quello al quale aveva chiesto di essere contattato (errore umano)
- CNIL (Francia) – caso SAN-2019-005 – Un URL non protetto (http invece che https) per condividere documenti contenenti dati personali viola l'art. 32 del GDPR (errore umano – configurazione)

Emerge chiaramente, anche dal punto di vista statistico, il fatto che l'errore umano rappresenti – allo stato – la causa predominante dei data breach portati all'attenzione delle Autorità di controllo. Nello specifico, l'errore umano più frequente è quello consistente nella scarsa attenzione ai contenuti oggetto di comunicazione o di diffusione online e alla effettiva base giuridica e legittimazione alla comunicazione o diffusione delle informazioni personali. Accanto a questo anche l'errore umano consistente in una erronea configurazione dei sistemi impiegati per il trattamento dei dati personali, rappresenta l'ulteriore fattore di rischio. I data breach determinati, invece, da un attacco esterno all'organizzazione del titolare del trattamento sono quelli consistenti nell'attacco con il malware di tipologia ransomware.

## 7 Le cause dei data breach

Secondo la definizione contenuta nel GDPR il data breach (o, violazione dei dati personali) consiste nella "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Riprendendo la definizione di data breach contenuta nel GDPR è evidente come le violazioni di dati personali possono ripartirsi in due tipologie generali: da un lato quelle in cui il data breach si è determinato "accidentalmente" e, dall'altro, quelle in cui gli effetti della violazione sono da ricondursi ad una qualche attività illecita. Nella prima categoria possiamo ricomprendere la forza maggiore e gli

errori umani mentre, nella seconda, tutte le attività di attacco che incidano in modo più o meno significativo sul processo di trattamento dei dati personali.

## 7.1 Forza Maggiore ed Errori Umani

Una delle prime cause dei data breach è, come abbiamo visto, determinata da errore umano. Questo può risolversi in diverse tipologie di data breach spesso in tutto o in parte associate ad errori nella configurazione degli strumenti informatici ma anche in errori nella gestione degli strumenti informatici; erronea formattazione e dismissione degli strumenti di memorizzazione delle informazioni; erronea gestione dei backup e loro compromissione; errori derivanti da omesso o ritardato aggiornamento delle vulnerabilità. Accanto agli errori umani non possono, però, non evidenziarsi anche i data breach dipendenti da cause di forza maggiore quali quelli legati all'interruzione della somministrazione di energia elettrica; eventi naturali che incidano sulla disponibilità delle informazioni memorizzate (quali, ad esempio, incendi, allagamenti etc).

## 7.2 Il malware (e il ransomware, in particolare)

I malware rappresentano una delle minacce più serie per i sistemi informatici, specialmente quando questi siano utilizzati per il trattamento di dati personali. Il termine 'malware' indica un'ampia categoria di software progettati specificamente per danneggiare, alterare o compromettere i sistemi informatici bersaglio. È importante notare che, sebbene comunemente si tenda a usare il termine 'virus informatico' per riferirsi a tutto il malware, in realtà i virus rappresentano solo una sottocategoria all'interno di questo vasto insieme. I malware possono colpire una varietà di dispositivi, tra cui computer, dispositivi mobili e tablet. Le loro finalità variano ampiamente: possono causare danni diretti ai sistemi, alterare o cancellare dati, introdursi abusivamente nei sistemi per sottrarre informazioni sensibili o per condurre attività illecite, come l'estorsione di denaro tramite ransomware. Data la loro natura versatile e la

continua evoluzione, i malware rappresentano una sfida costante per la sicurezza informatica e richiedono un'attenzione continua e misure di protezione aggiornate.

Tra le varie categorie di malware, i **ransomware** occupano una posizione particolarmente perniciosa. Questi software malevoli, una volta infiltrati nel sistema operativo bersaglio, ne alterano il funzionamento o limitano l'accesso ai documenti in esso contenuti. Il loro obiettivo principale è richiedere un riscatto in denaro, spesso sotto forma di valuta virtuale come i bitcoin, in cambio della restituzione dell'accesso o del ripristino delle funzionalità del dispositivo.

Le modalità attraverso cui il malware, inclusi i ransomware, viene veicolato fino al suo bersaglio possono variare, ma la più comune è tramite l'uso di allegati malevoli in e-mail di phishing. Queste e-mail sono spesso confezionate con grande attenzione ai dettagli per ingannare i destinatari. Ad esempio, possono convincere il destinatario che cliccando su un link all'interno dell'e-mail potrà verificare lo stato di consegna di un pacco, scaricare una fattura per una prestazione ricevuta, o accedere ad altre informazioni di interesse apparente.

Queste tecniche di social engineering si basano sulla capacità di convincere la vittima a cliccare su un allegato o un link, sfruttando vari stratagemmi psicologici. Si può indurre la vittima a credere che cliccando sull'allegato otterrà un vantaggio, eviterà perdite economiche, o accederà a un documento di particolare rilevanza. Queste strategie truffaldine sono estremamente efficaci perché sfruttano la curiosità, la paura o l'urgenza percepite dal destinatario.

La modalità di azione tipica dei ransomware è rendere inaccessibili i file della vittima attraverso la cifratura. La vittima si trova quindi di fronte alla necessità di pagare un riscatto per ottenere la chiave di decriptazione e recuperare l'accesso ai propri dati. Ovviamente l’eventuale pagamento del riscatto in denaro non implica necessariamente la possibilità che la vittima ottenga effettivamente i

codici in grado di ripristinare il sistema informatico allo stato precedente all'attacco ad opera del ransomware.

Una tattica più recente e preoccupante nel panorama dei ransomware è quella della 'double extortion' o doppia estorsione. In questo scenario, oltre a richiedere un pagamento per la decrittazione dei file, gli attaccanti minacciano di divulgare pubblicamente i dati cifrati se non viene pagato un ulteriore riscatto. Questa strategia aumenta notevolmente la pressione sulla vittima, che si trova a dover gestire non solo la perdita di accesso ai propri dati, ma anche il rischio di esposizione di informazioni sensibili o confidenziali.

Prevenire il contagio da ransomware può essere una sfida complessa, specialmente in ambienti di rete dove non tutti gli utenti sono pienamente consapevoli dei rischi informatici. Tuttavia, esistono diverse misure efficaci per mitigare il rischio associato agli attacchi ransomware:

1. **Aggiornamenti costanti**: È cruciale mantenere i sistemi operativi e i software sempre aggiornati. Gli aggiornamenti spesso includono patch di sicurezza che possono prevenire vulnerabilità note.
2. **Backup efficaci**: Un sistema di backup ben gestito, telematicamente protetto e isolato dai dati originali, è fondamentale. Questo assicura la disponibilità di copie sicure dei dati in caso di attacco.
3. **Formazione dei dipendenti**: Educare adeguatamente i dipendenti sui rischi e su come riconoscere attacchi di phishing e altre tattiche utilizzate dai ransomware è essenziale.
4. **Uso della cifratura**: La cifratura dei dati personali è una tecnica di minimizzazione che rende i dati meno accessibili in caso di violazione. Questo sistema rende inefficace l'eventuale minaccia di diffondere online i contenuti attaccati dal ransomware (in quanto si tratterebbe di informazioni comunque rese inaccessibili dal titolare.
5. **Antivirus e aggiornamenti**: È importante dotare i sistemi che trattano dati personali di un software antivirus robusto e mantenerlo costantemente aggiornato.
6. **Endpoint security**: Un approccio di 'endpoint security' prevede sistemi integrati in grado di identificare comportamenti anomali all'interno della rete. Questi sistemi possono bloccare attività

potenzialmente dannose, anche di malware non ancora noti, che un antivirus tradizionale potrebbe non rilevare.

Incorporando queste misure, le organizzazioni possono ridurre notevolmente la probabilità e l'impatto di un attacco ransomware.

## 7.3 Il social engineering

Il termine 'social engineering' (o ingegneria sociale) si riferisce a una serie di tecniche utilizzate in attività che spesso mirano a compromettere i sistemi informatici. L'obiettivo principale di queste tecniche non è tanto il sistema informatico in sé, quanto piuttosto gli utenti che lo utilizzano. L'ingegneria sociale sfrutta le debolezze umane, come la fiducia, la curiosità o la paura, per manipolare gli individui a compiere azioni che possono mettere a rischio la sicurezza dei sistemi.

Ad esempio, un attaccante che intenda prendere di mira i sistemi informatici di un ente pubblico potrebbe raccogliere informazioni utili a bypassare anche sistemi ben protetti dal punto di vista tecnico. La vera debolezza potrebbe risiedere nei dipendenti dell'ente, che potrebbero essere ingannati per ottenere credenziali di accesso o utilizzati come vettori per introdurre malware nel sistema. Questo potrebbe avvenire tramite e-mail di phishing, telefonate fraudolente, chiavette USB veicolo del malware inserite incautamente (o anche inconsapevolmente dal dipendente che l’abbia, ad esempio, rinvenuta nei pressi dell’edificio dell’ente) nei sistemi informativi della vittima o altre tattiche che mirano a ottenere informazioni sensibili o ad indurre comportamenti rischiosi.

Quindi, mentre la sicurezza informatica si concentra spesso sugli aspetti tecnici, l'ingegneria sociale si rivolge all'elemento umano, sfruttandolo come un punto debole nel complesso sistema di difesa di un'organizzazione.

Data la natura particolarmente insidiosa degli attacchi basati su tecniche di social engineering, si ritiene che l'approccio più efficace per contrastarli sia la formazione continua e approfondita dei

dipendenti in materia di sicurezza informatica. Questa formazione non dovrebbe limitarsi a fornire informazioni sui vari tipi di attacchi, ma dovrebbe anche includere l'addestramento su come riconoscere e reagire a tentativi di ingegneria sociale.

La formazione dovrebbe essere un processo dinamico e adattivo, in grado di evolversi insieme alle tecniche utilizzate dagli attaccanti. Ciò include la simulazione di attacchi di phishing, l'educazione sui segnali di pericolo di comunicazioni sospette e l'addestramento su procedure da seguire in caso di sospetto attacco. Inoltre, è essenziale creare una cultura in cui la sicurezza viene considerata una responsabilità collettiva, incoraggiando i dipendenti a comunicare immediatamente eventuali sospetti e a segnalare incidenti di sicurezza senza timore di ripercussioni.

In conclusione, mentre gli strumenti tecnologici giocano un ruolo fondamentale nella protezione dai rischi informatici, l'istruzione e la consapevolezza dei dipendenti sono altrettanto cruciali per mitigare efficacemente il rischio di attacchi basati su tecniche di social engineering.

## 7.4 Phishing e spear-phishing

Si è già discusso dei rischi legati alle e-mail di phishing, che rappresentano una minaccia sia per le risorse economiche di un'Amministrazione o dei singoli dipendenti, sia come potenziali veicoli per la diffusione di malware, con conseguenti impatti negativi sui sistemi informatici bersaglio.

Il phishing è comunemente definito come una tecnica di attacco di “pesca a strascico”, in cui il malintenzionato non mira a un singolo individuo specifico, ma piuttosto invia lo stesso messaggio truffaldino a numerosi destinatari contemporaneamente. Queste e-mail sono confezionate in modo ingannevole per sembrare legittime e spesso imitano comunicazioni provenienti da fonti affidabili, come istituzioni finanziarie, aziende note o enti governativi. L'obiettivo è indurre il destinatario a cliccare su allegati o seguire link contenuti nell'email,

che possono condurre al download di malware o a pagine web fraudolente progettate per sottrarre informazioni sensibili, come credenziali di accesso o dati finanziari.

È importante sottolineare che, nonostante la natura 'non mirata' di questi attacchi, le tecniche di ingegneria sociale utilizzate nelle e-mail di phishing sono spesso sofisticate e possono facilmente ingannare anche utenti esperti. Pertanto, la consapevolezza e la formazione continua su come riconoscere e gestire tali minacce sono fondamentali per la sicurezza informatica.

Lo "spear phishing" è una forma più sofisticata e mirata di phishing. Mentre il phishing tradizionale consiste nell'invio di messaggi ingannevoli a un ampio numero di destinatari in modo indiscriminato, lo spear phishing si concentra su individui o organizzazioni specifiche. Questa tecnica richiede una preparazione e una ricerca più approfondite da parte dell'attaccante, che raccoglie informazioni dettagliate sui suoi bersagli per rendere il tentativo di inganno il più convincente possibile.

In uno spear phishing, l'e-mail o il messaggio truffaldino è spesso personalizzato per adattarsi ai dettagli conosciuti del destinatario, come il nome, la posizione lavorativa, i colleghi, le abitudini di lavoro e gli interessi personali. Questo rende il messaggio molto più convincente e aumenta la probabilità che la vittima cada nella trappola. Ad esempio, un'email di spear phishing potrebbe imitare la comunicazione di un collega, di un superiore, o di un'altra entità fidata, richiedendo azioni urgenti, come il trasferimento di fondi, la condivisione di password o l'accesso a informazioni sensibili.

L'obiettivo finale dello spear phishing è spesso quello di ottenere accesso non autorizzato a sistemi informatici, sottrarre dati sensibili, installare malware o compiere frodi finanziarie. A causa del suo alto livello di personalizzazione e apparente legittimità, lo spear phishing rappresenta una minaccia significativa e richiede un'attenzione particolare e misure di sicurezza avanzate, come (ancora una volta) la

formazione degli utenti a riconoscere segnali sospetti e l'implementazione di soluzioni di sicurezza email sofisticate.

# 8 Alcune precauzioni

## 8.1 Dispositivi BYOD

BYOD è l'acronimo di 'Bring Your Own Device', una politica adottata da aziende private e enti pubblici che permette ai dipendenti o agli utenti di usare i propri dispositivi personali (come computer, tablet e smartphone) per scopi lavorativi. Questo consente loro di accedere alle informazioni o ai dati dell'organizzazione. Se da un lato il BYOD può generare un risparmio per l'organizzazione, evitando l'acquisto di dispositivi aziendali per i dipendenti, dall'altro introduce potenziali rischi di sicurezza. Questi rischi sono dovuti alla difficoltà dell'ente o dell'azienda di controllare le vulnerabilità o i malware che possono essere presenti sui dispositivi personali.

Di BYOD si occupa anche il Codice dell'amministrazione digitale, all'art. 12 che reca le norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa. Nel comma 3-bis, in particolare, si prevede che le PPAA "favoriscono l'uso da parte dei lavoratori di dispositivi elettronici personali o, se di proprietà dei predetti soggetti, personalizzabili, al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo". In caso di uso di dispositivi elettronici personali, le PPAA, "nel rispetto della disciplina in materia di trattamento dei dati personali, adottano ogni misura atta a garantire la sicurezza e la protezione delle informazioni e dei dati, tenendo conto delle migliori pratiche e degli standard nazionali, europei e internazionali per la protezione delle proprie reti, nonché a condizione che sia data al lavoratore adeguata informazione sull'uso sicuro dei dispositivi, anche attraverso la diffusione di apposite linee guida, e disciplinando, tra l'altro l'uso di webcam e microfoni, previa informazione alle organizzazioni sindacali". Dalla norma in esame emerge la necessità – nel caso in cui si ammetta il dipendente ad impiegare in ambito

lavorativo strumenti BYOD – sia di garantire il rispetto dei principi in materia di protezione dei dati personali (non soltanto del lavoratore ma anche degli interessati i cui dati personali sia stato autorizzato a trattare nell'interesse del titolare del trattamento dei dati personali) sia a garantire che l'introduzione di uno strumento, come il BYOD, "estraneo" all'amministrazione e di proprietà del lavoratore, possa rappresentare, per l'Amministrazione, il veicolo di rischi per la sicurezza e la protezione delle informazioni e dei dati dell'Amministrazione medesima. Il BYOD, infatti, che non sia precedentemente approntato all'uso all'interno dei sistemi informatici e telematici dell'ente mediante la verifica della presenza di eventuali vulnerabilità, malware etc. può rappresentare un rischio per l'integrità, confidenzialità e disponibilità delle informazioni della PA.

I rischi associati all'utilizzo di politiche BYOD (Bring Your Own Device) all'interno di una pubblica amministrazione possono essere sostanziali, data la natura sensibile delle informazioni gestite. Tra i principali rischi possono elencarsi:

- **Sicurezza dei dati**: I dispositivi personali potrebbero non avere le stesse misure di sicurezza dei dispositivi forniti dall'amministrazione. Ciò determina un incremento del rischio sui dati della PA.
- **Vulnerabilità ai malware**: I dispositivi personali potrebbero essere più esposti a malware e virus, che possono compromettere non solo il dispositivo stesso ma anche la rete dell'ente pubblico quando vi si collegano.
- **Mancanza di controllo IT**: È difficile per i reparti IT monitorare e mantenere aggiornati tutti i dispositivi personali – nel caso in cui i BYOD non debbano essere preventivamente analizzati, (eventualmente) bonificati e configurati per poter essere impiegati all'interno della rete dell'Ente – il che aumenta il rischio di vulnerabilità.
- **Perdita o furto dei dispositivi**: I dispositivi personali usati per il lavoro possono contenere dati personali nella titolarità della PA. Se un dispositivo venisse perso o rubato, e contenesse dati personali di cui è titolare l'ente

presso il quale il dipendente lavora, l'evento dovrebbe essere segnalato al titolare il quale dovrà avviare le procedure di gestione del data breach (mediante la notifica al Garante, l'eventuale comunicazione agli interessati etc).

- **Conflitti di compatibilità e standardizzazione**: I vari dispositivi possono avere sistemi operativi e software diversi, creando problemi di compatibilità e rendendo più complessa la gestione.

Per mitigare questi rischi, le pubbliche amministrazioni che adottano politiche BYOD dovrebbero implementare strategie di sicurezza adeguate, tra cui la gestione dei dispositivi mobili (MDM), l'addestramento dei dipendenti sulla sicurezza informatica e la definizione di politiche chiare sull'uso dei dispositivi personali. In particolare, prima di introdurre dispositivi BYOD, dovrebbero essere effettuati gli opportuni controlli al fine di garantire la protezione dei dati dell'ente e la confidenzialità delle informazioni veicolate.

## 8.2 Reti WI-FI

Anche le reti Wi-Fi possono essere veicolo di attacco o di infezione dei dispositivi connessi a quella medesima rete. In particolare, esistono delle tecniche di attacco che consistono nel simulare una rete Wi-Fi dell'Ente pubblico in modo da dirottare o captare i contenuti degli ignari "navigatori" che non si accorgono di non essere connessi alla rete "dell'Ente" ma a una rete Wi-Fi creata appositamente con finalità malevole.

## 8.3 Vulnerabilità ed aggiornamento dei sistemi

Con riferimento alle misure di sicurezza che ciascun titolare o responsabile del trattamento dovrebbe adottare è essenziale ribadire che il GDPR non ne individua di specifiche ma impone a tali soggetti di compiere una valutazione approfondita dei rischi e, conseguentemente, di apprestare le "difese" adeguate che siano necessarie a rendere il rischio accettabile. Per questo motivo non

esistono più cataloghi normativi o regolamentari di misure di sicurezza da adottare, posto che ciascun soggetto obbligato dovrà individuare le misure in base a numerosi parametri. Esistono, tuttavia, delle misure che sono ritenute utili a priori. Una di queste è quella che impone un aggiornamento costante del software a disposizione.

È importante comprendere, inoltre, che le politiche di sicurezza su qualsiasi sistema informatico non possono mai ritenersi un "punto d'arrivo" posto che vengono continuamente individuate le vulnerabilità di dispositivi, sistemi operativi o software e che queste possono essere sfruttate dagli attaccanti. Non si potrà mai, pertanto, avere una situazione di "sicurezza assoluta" dal punto di vista informatico ma si dovrà costantemente lavorare per garantire l'aggiornamento dei sistemi e delle misure di protezione (siano essi hardware o software come firewall, sistemi antintrusione, antivirus, etc.). L'aggiornamento dei sistemi operativi è essenziale e deve essere costantemente monitorato.

Occorre, tuttavia, considerare che in un sistema informatico complesso in cui operino differenti tipologie di dispositivi, differenti tipologie di sistemi operativi e software, e in cui si intersechino le attività di tali differenti sistemi è ben possibile - e anzi non è infrequente - che a un aggiornamento di uno di tali sistemi possa conseguire la mancanza di interoperabilità o di funzionamento di altri sistemi collegati. Questo problema è determinato proprio dal fatto che non sempre i sistemi sono interoperabili e compatibili tra di loro e, ad esempio, un software gestionale dell'Amministrazione, una volta aggiornati i sistemi operativi sui quali questo software viene utilizzato, potrebbe smettere di funzionare perché non riconosce l'ambiente in cui si trova a operare.

Al fine di evitare questo tipo di problemi è necessario affidare la gestione e l'aggiornamento dei sistemi istituzionali a soggetti effettivamente competenti. Ricordiamo, inoltre, che scegliere soggetti esterni realmente competenti alla gestione o aggiornamento dei dati (anche personali) in essi contenuti può essere rilevante in sede di

scelta del Responsabile esterno del trattamento (ai sensi dell'art. 28 del GDPR).

## 8.4 I sistemi di backup

Già il "vecchio" Codice della Privacy (ossia il D.Lgs. 196/2003 prima della modifica apportata dal D.Lgs. 101/2018) riconosceva l'importanza delle misure di backup come strumento essenziale per prevenire le perdite di dati accidentali o causate da attacchi mirati ai sistemi informatici. Il processo di backup implica la creazione di copie, sia integrali che incrementali, dei dati presenti sui dispositivi di memorizzazione. Queste copie sono progettate per consentire un ripristino rapido ed efficiente dei dati in caso di cancellazione accidentale o a seguito di un attacco, come quello perpetrato tramite ransomware.

Il backup è una componente fondamentale della strategia di sicurezza informatica e di gestione dei rischi. Non si tratta solo di creare copie dei dati, ma anche di garantire la loro conservazione in modo sicuro e accessibile. Questo richiede l'attuazione di politiche di conservazione dei dati ben definite, che includano l'identificazione della frequenza dei backup, la scelta di soluzioni di memorizzazione affidabili e sicure, e la definizione di procedure per il test e il ripristino dei dati da queste copie di sicurezza.

Un aspetto critico di una buona strategia di backup è assicurare che le copie di sicurezza siano conservate in una posizione separata dal sistema originale, preferibilmente in un ambiente diverso (come il cloud o un data center remoto), per proteggerli contro danni fisici, furti o altri disastri (ma anche per proteggerli dalle stesse violazioni che potrebbero coinvolgere le informazioni da sottoporre a backup: se il sistema di backup fosse nel medesimo locale del sistema da sottoporre a backup, in caso di incendio, ad esempio, sarebbero coinvolti entrambi i sistemi informatici). Inoltre, è essenziale che le copie di backup siano criptate e protette da accessi non autorizzati per mantenere la riservatezza e l'integrità dei dati.

In conclusione, l'adozione di sistemi di backup adeguati e di politiche di conservazione efficaci è cruciale per garantire la resilienza dei sistemi informatici e la protezione dei dati, in linea con le direttive del Codice della Privacy e con le migliori pratiche di sicurezza informatica.

## 8.5 La cifratura

Le tecniche di cifratura, basate su vari algoritmi, sono strumenti fondamentali per garantire l'inaccessibilità delle informazioni a soggetti non autorizzati. Questi algoritmi si dividono principalmente in due categorie: algoritmi a chiave simmetrica e algoritmi a chiave asimmetrica.

- **Algoritmi a Chiave Simmetrica**: In questa tipologia, lo stesso algoritmo e la stessa chiave vengono utilizzati sia per cifrare che per decifrare i contenuti. Questo metodo è efficiente, ma richiede che entrambe le parti condividano la chiave in modo sicuro.
- **Algoritmi a Chiave Asimmetrica**: Invece, gli algoritmi a chiave asimmetrica utilizzano una coppia di chiavi – una pubblica e una privata. La chiave pubblica è usata per cifrare i dati, mentre la chiave privata è necessaria per decifrarli.

Nella seconda tipologia rientrano, ad esempio, i sistemi di cifratura basati sull'uso della firma digitale. Qualora il mittente intenda inviare telematicamente, anche avvalendosi di un sistema "non sicuro" di comunicazione (quale, ad esempio, l'email) un documento in modo da assicurarsi che solo l'effettivo destinatario possa accedere al contenuto potrà utilizzare il software di gestione della firma digitale per cifrare il documento. Tale software chiederà al mittente di ricercare la chiave pubblica della relativa firma digitale del destinatario al fine di criptare il documento. Una volta criptato potrà essere allegato e inviato al destinatario il quale, utilizzando la chiave privata della firma digitale, potrà decriptare il documento cifrato con la relativa chiave pubblica.

Allo stesso modo un soggetto potrebbe voler inserire un documento all'interno di un dispositivo portatile (come, ad esempio, una pennina USB) ed essere sicuro che, dovendosi spostare dal posto A (ad esempio dal luogo di lavoro) al posto B (ad esempio la propria abitazione), qualora dovesse smarrire la pennina USB nessuno possa accedere ai contenuti del documento memorizzato sulla medesima pennina USB. Per far ciò potrà utilizzare la chiave pubblica della propria firma digitale per cifrare il documento mentre si trova nel posto A e, poi, una volta giunto nel posto B, decifrare il documento utilizzando la chiave privata della propria firma digitale.

Si noti che il GDPR fa spesso riferimento alla cifratura come uno dei possibili strumenti per assicurare l'esistenza di garanzie adeguate nella protezione dei dati (ad esempio si veda l'art. 6, par. 4, lett. e, oppure, ancora, l'art. 32, par. 1, o l'art. 34, par. 3, lett. a). Inoltre, il Considerando 83, in modo ancor più esplicito, prevede che "*per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura*".

## 8.6 La dismissione dell'hardware e la cancellazione dei dati

Un importante aspetto da considerare durante la dismissione di sistemi di memorizzazione delle informazioni è la necessità di una cancellazione sicura dei dati dai dispositivi. È infatti noto che la semplice eliminazione dei file attraverso il 'cestino' del sistema operativo non rimuove effettivamente le informazioni dal supporto di memorizzazione. I dati cancellati in questo modo possono spesso essere recuperati con strumenti specializzati, rappresentando così un potenziale rischio di violazione dei dati (data breach).

Pertanto, prima di dismettere hardware come memorie USB, hard disk di computer, smartphone e altri dispositivi di memorizzazione, è essenziale adottare metodi di cancellazione sicura dei dati (conosciuti

come 'wiping'). Questi metodi assicurano che i dati vengano rimossi in modo definitivo e irrecuperabile dal dispositivo.

Il processo di wiping implica la sovrascrittura dei dati presenti nel dispositivo con serie di dati casuali o con un pattern specifico, più volte e in maniera tale da rendere impossibile il loro recupero. Esistono diversi standard e software specializzati per la cancellazione sicura dei dati, alcuni dei quali soddisfano requisiti di sicurezza governativi o militari.

Adottare procedure di cancellazione sicura dei dati è un passo fondamentale per proteggere le informazioni sensibili e per conformarsi alle normative sulla privacy e sulla protezione dei dati, come il GDPR, che richiedono misure adeguate per prevenire l'accesso non autorizzato ai dati personali.

## 8.7 Le policy sulla sicurezza informatica

Un efficace metodo per aumentare il livello di consapevolezza sui rischi informatici tra i dipendenti di un ente è la creazione di un documento che delinei le politiche di sicurezza informatica adottate dall'ente stesso. Tale processo inizia con un'accurata valutazione delle aree, dei dispositivi e degli strumenti più vulnerabili a rischi informatici. Questa analisi dovrebbe essere condotta con la collaborazione di personale specializzato in sicurezza informatica.

Una volta identificate le aree a rischio, il documento dovrebbe descrivere dettagliatamente le misure preventive da adottare per evitare incidenti informatici, nonché le strategie di contenimento e risposta da attuare in caso di incidente. Queste policy sulla sicurezza informatica dovrebbero essere distribuite e rese accessibili a tutti i membri dell'amministrazione.

In particolare, le policy possono offrire un'opportunità per definire chiaramente le istruzioni e le linee guida per i dipendenti che utilizzano strumenti informatici (come computer, tablet e smartphone) nell'ambito del loro lavoro. Queste istruzioni dovrebbero coprire i rischi informatici più comuni e fornire indicazioni su come

gestire in modo sicuro tali dispositivi, includendo pratiche come l'uso di password forti, il riconoscimento di tentativi di phishing e le procedure per segnalare eventuali violazioni della sicurezza.

L'obiettivo di queste policy è quindi di creare una cultura della sicurezza informatica all'interno dell'ente, dove ogni dipendente è consapevole dei rischi e sa come agire in modo responsabile per proteggere sia le proprie informazioni che quelle dell'organizzazione.

# 9 Casi di studio

## 9.1 Pubblicazioni obbligatorie in materia di trasparenza

Il rapporto tra privacy e trasparenza nella Pubblica Amministrazione è caratterizzato da un equilibrio delicato. Da un lato, le pubbliche amministrazioni possono diffondere dati personali trattati nell'ambito dell'esecuzione di compiti di interesse pubblico o in relazione all'esercizio di pubblici poteri, ma questo è permesso solo se espressamente previsto da specifiche disposizioni di legge, regolamenti o atti amministrativi generali (art. 2-ter D.Lgs. 196/2003). Dall'altro lato, le Pubbliche Amministrazioni sono soggette a obblighi di pubblicazione dettati dal principio di trasparenza, come stabilito dal D.Lgs. 33/2013 (il cosiddetto “Decreto Trasparenza”). Questo principio impone la divulgazione di specifici documenti, informazioni o dati per garantire la trasparenza delle attività amministrative e la partecipazione attiva dei cittadini mediante forme di controllo diffuso sull’attività della PA.

Tuttavia, nell'adempiere a questi obblighi di pubblicazione, le amministrazioni devono operare nel rispetto dei principi relativi alla protezione dei dati personali. Questo significa bilanciare il diritto alla privacy degli individui con l'interesse pubblico alla trasparenza e all'accesso alle informazioni. Le Linee guida del Garante per la Protezione dei Dati Personali del 2014, pur in un contesto normativo

che si è evoluto nel tempo, continuano a fornire indicazioni rilevanti su come gestire questo equilibrio. Abbiamo visto come una rilevante percentuale dei data breach delle Amministrazioni sia causata da errori nella diffusione delle informazioni personali. L'ambito della trasparenza rappresenta anche un settore sul quale occorre concentrare gli sforzi formativi dell'Amministrazione che non devono considerare unicamente i singoli obblighi di trasparenza mediante la pubblicazione sul sito istituzionale ma anche (e soprattutto) la corretta interpretazione delle norme sul versante della protezione dei dati personali.

In sintesi, la Pubblica Amministrazione deve agire con cautela, garantendo che qualsiasi divulgazione di dati personali avvenga nel rispetto della normativa sulla privacy e delle necessità di trasparenza, contribuendo così a costruire una società più informata e responsabile.

Il Codice della Privacy, come modificato dal D. Lgs. 101/2018, ha sostanzialmente confermato l'assetto normativo precedente. L'art. 2-ter, comma 3, infatti, prevede che la diffusione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, sia ammessa soltanto quando prevista da legge, regolamento o atto amministrativo generale o se necessaria per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri, mentre l'art. 2-septies, comma 8, stabilisce un generale divieto di diffusione dei dati genetici, biometrici e relativi allo stato di salute.

In sintesi, le pubbliche amministrazioni possono diffondere dati personali solo laddove vi sia una norma di legge o di regolamento o un atto amministrativo generale che, determinando l'ambito del compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ne delimiti anche le ipotesi di diffusione, mentre non possono mai diffondersi dati idonei a rivelare lo stato di salute.

Ma, anche in presenza di un'ipotesi legittimante la diffusione, occorre sempre valutare quali dati personali siano pertinenti e

adeguati rispetto alle finalità perseguite, evitando accuratamente le diffusioni di dati personali non rispettose del principio di minimizzazione di cui all'art. 5, comma 1, lett. c) del GDPR, o che vengano mantenute sul sito dell'Amministrazione per un tempo più lungo di quanto previsto dalla norma che impone la pubblicazione stessa.

Occorre, poi, avere a mente che non tutte le pubblicazioni sul sito istituzionale di un ente pubblico perseguono le finalità indicate dall'art. 1 del Decreto Trasparenza. Oltre alle pubblicazioni per finalità di trasparenza (nella sezione "Amministrazione Trasparente"), infatti, possono esservi pubblicazioni che trovano il loro fondamento in altri ambiti normativi (ad esempio nel Testo Unico Enti Locali) e perseguono differenti finalità (ad esempio pubblicità integrativa dell'efficacia, pubblicità notizia e, in genere, pubblicità legale). Tali pubblicazioni, normalmente fatte attraverso lo strumento dell'Albo online (si veda, al proposito, l'art. 32, L. 18 giugno 2009, n. 69), comportano una serie di ulteriori problematiche, con riguardo ai data breach. Le regole tecniche che disciplinano l'albo online differiscono da quelle previste dal D.Lgs. 33/2013 per le pubblicazioni per finalità di trasparenza. Le pubblicazioni nell'albo online, ad esempio, non devono essere indicizzabili dai motori di ricerca generalisti (a differenza delle informazioni pubblicate nella sezione "Amministrazione Trasparente" che, invece, devono essere indicizzabili dai motori di ricerca). Le pubblicazioni nell'albo online, inoltre, analogamente a quanto avviene per le pubblicazioni previste dal Decreto Trasparenza, non prevede una sezione "archivio" attraverso la quale mettere a disposizione i documenti per i quali sia scaduto il periodo di pubblicazione (normalmente di 15 giorni in ossequio a quanto previsto dal TUEL). Sia la indicizzazione delle informazioni da parte dei motori di ricerca (con la possibilità di rendere ricercabili online quelle informazioni per le quali sia decorso il periodo di pubblicazione) sia la diffusione di dati personali oltre il termine di pubblicazione per finalità di pubblicità legale, rappresentano ipotesi di data breach.

### 9.1.1 L’art. 7-bis del D.Lgs. 33/2013

Il D. Lgs. 33/2013 impone alle pubbliche amministrazioni e ai soggetti tenuti al rispetto della normativa sulla trasparenza una serie di obblighi di pubblicazione di informazioni, dati e documenti sui propri siti istituzionali, e prevede, in caso di omesso adempimento, la possibilità in capo a chiunque sia interessato di presentare istanza di accesso civico (art. 5, comma 1, D.Lgs. 33/2013) per ottenere la pubblicazione dei dati, informazioni e documenti. Lo scopo perseguito dal Decreto Trasparenza è la trasparenza (intesa come “accessibilità totale dei dati e delle informazioni”) e la conoscibilità per i cittadini dell’organizzazione e delle attività delle pubbliche amministrazioni, anche al fine di contrastare la corruzione all’interno della Pubblica Amministrazione stessa, nel rispetto della disciplina in materia di protezione dei dati personali.

L’art. 7-bis, rubricato “Riutilizzo dei dati pubblicati", al comma IV prevede che: “nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione”.

L’art. 7-bis regola, dunque, i rapporti delle pubblicazioni per finalità di trasparenza con la disciplina in materia di protezione dei dati personali, stabilendo una serie di regole, coerenti anche con le modifiche apportate al Codice Privacy.

### 9.1.2 In particolare: la corretta pubblicazione dei curriculum vitae

Il D. Lgs. 33/2013 prevede all’art. 15, fra le altre cose, l’obbligo di pubblicazione per le pubbliche amministrazioni dei curriculum professionali concernenti i titolari di incarichi di collaborazione o consulenza, nei limiti dei dati pertinenti alle finalità di trasparenza perseguite e da effettuarsi entro tre mesi dal conferimento dell’incarico e per i tre anni successivi alla cessazione dell’incarico. In base alle indicazioni del Garante è consentita la pubblicazione dei soli

dati personali la cui diffusione sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto. Bisogna pertanto provvedere all'oscuramento delle informazioni che risultano eccedenti o non pertinenti rispetto alla finalità di trasparenza.

Sono pertinenti dati relativi ai titoli di studio e professionali o relativi alle esperienze lavorative, le conoscenze linguistiche o informatiche, la partecipazione a seminari, convegni o le pubblicazioni. Viceversa, sono dati eccedenti il codice fiscale, l'indirizzo o il recapito telefonico personale. Di questi ultimi non è consentita la pubblicazione e il titolare è tenuto ad attenta verifica del contenuto del curriculum. Una eventuale pubblicazione dei curriculum che ecceda i principi di minimizzazione dei dati personali nelle pubblicazioni per finalità di trasparenza integra, a tutti gli effetti, una violazione di dati personali (o, data breach).

## 9.2 Pubblicazione dei "dati ulteriori" e anonimizzazione

Come visto precedentemente, la diffusione di dati personali da parte delle pubbliche amministrazioni è consentita solo in presenza di una base giuridica adeguata (art. 2-ter Codice privacy). Oltre a ciò, il Decreto Legislativo 33/2013 prevede disposizioni specifiche per la pubblicazione di 'dati ulteriori', ovvero di dati per i quali non esiste un obbligo specifico di pubblicazione.

Secondo l'articolo 7-bis, comma 3, del D. Lgs. 33/2013, dati, informazioni e documenti che non sono soggetti a un obbligo di pubblicazione possono essere pubblicati solo dopo che i dati personali in essi contenuti siano stati resi anonimi. La corretta anonimizzazione dei dati implica che questi vengano trattati in modo tale da impedire qualsiasi possibilità di identificazione delle persone a cui si riferiscono originariamente. Questa operazione deve garantire che non sia in alcun modo possibile risalire agli interessati.

Questa norma ha un'ampia portata e si applica non solo ai dati pubblicati nella sezione 'Amministrazione Trasparente' dei siti delle pubbliche amministrazioni, ma a qualsiasi tipo di dato ulteriore che si voglia rendere pubblico. Ciò sottolinea l'importanza di una gestione responsabile e conforme alla normativa vigente dei dati personali, anche quando non sussiste un obbligo specifico di pubblicazione, per assicurare la protezione della privacy dei cittadini. La corretta applicazione dei criteri di anonimizzazione implica il coinvolgimento di soggetti esperti quali, anzitutto, il DPO dell'ente.

## 9.3 Data breach e accesso generalizzato

L'accesso generalizzato, noto anche come FOIA (Freedom of Information Act), introdotto dall'art. 5 comma II del D. Lgs. 33/2013 ed entrato in vigore il 23 dicembre 2016, rappresenta un diritto significativo nell'ambito della trasparenza pubblica. Esso consente a chiunque di accedere ai dati e documenti detenuti dalle pubbliche amministrazioni, promuovendo il controllo sulle funzioni istituzionali e l'utilizzo delle risorse pubbliche, nonché la partecipazione al dibattito pubblico.

Questo diritto, naturalmente, è soggetto a limitazioni, al fine di bilanciarlo con altri interessi. Queste limitazioni sono contenute nell'art. 5-bis, che prevede delle esclusioni assolute (contenute al comma 3) e delle esclusioni relative (al comma 2).

Ci limiteremo a esaminare quelle rilevanti in ordine al rapporto tra trasparenza e privacy, sottolineando come il Codice della Privacy, all'art. 59, comma 1-bis (introdotto dal D. Lgs. 101/2018) chiarisce che i presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restino disciplinati proprio dal D. Lgs. 33/2013.

Occupandoci prima delle esclusioni assolute rilevanti in tema di trattamento di dati personali, dobbiamo menzionare i dati inerenti allo stato di salute e alla vita sessuale, nonché i dati da cui possa inferirsi un disagio economico e sociale: essi rientrano tra i dati per i quali vige un divieto assoluto di ostensione a seguito di accesso generalizzato.

L’art. 5-bis del D. Lgs. 33/2013, al secondo comma, lett. a) prevede invece un’esclusione relativa, che stabilisce come l’accesso generalizzato possa essere rifiutato se il diniego risulti necessario per evitare un pregiudizio concreto alla protezione dei dati personali. Si consideri, inoltre, che qualora l’istanza di accesso generalizzato venga negata o differita a causa di un presunto “pregiudizio concreto” alla protezione dei dati personali, nell’eventuale fase di riesame del provvedimento, di fronte al Responsabile della Prevenzione della Corruzione e della Trasparenza - RPCT (ai sensi dell’art. 5, comma 7, del D. Lgs. 33/2013) quest’ultimo dovrà, prima di assumere le proprie decisioni in merito al riesame, contattare il Garante per la protezione dei dati personali, il quale dovrà rispondere entro dieci giorni. Occorre quindi trovare un bilanciamento tra la trasparenza come accessibilità totale e la tutela dei dati personali, sulla base del GDPR e del novellato Codice della Privacy.

Le prime indicazioni sul bilanciamento tra privacy e trasparenza possono ricavarsi dalla Determinazione n. 1309 del 28/12/2016 dell’ANAC, nella quale si afferma che “con riferimento alle istanze di accesso generalizzato aventi a oggetto dati e documenti relativi a (o contenenti) dati personali, l’ente destinatario dell’istanza deve valutare, nel fornire riscontro motivato a richieste di accesso generalizzato, se la conoscenza da parte di chiunque del dato personale richiesto arreca (o possa arrecare) un pregiudizio concreto alla protezione dei dati personali, in conformità alla disciplina legislativa in materia. La ritenuta sussistenza di tale pregiudizio comporta il rigetto dell’istanza, a meno che non si consideri di poterla accogliere, oscurando i dati personali eventualmente presenti e le altre informazioni che possono consentire l’identificazione, anche indiretta, del soggetto interessato”.

Nella stessa determinazione, sono poi individuati una serie di criteri che le pubbliche amministrazioni devono tenere presenti, ai fini della valutazione del pregiudizio concreto. Utili indicazioni possono ricavarsi anche dai plurimi pareri che il Garante Privacy ha emanato in

tema di istanze di accesso generalizzato, disponibili sul sito dell'Autorità, nella sezione "provvedimenti".

## 9.4 Accesso documentale (L. 241/90) e trattamento dei dati personali

Abbiamo precedentemente discusso l'accesso generalizzato come introdotto dal Decreto Legislativo 33/2013, ma è importante anche considerare l'accesso documentale 'ordinario' secondo la Legge 241/1990. L'articolo 86 del GDPR, infatti, consente la comunicazione di dati personali contenuti in documenti ufficiali, nel rispetto del diritto dell'Unione o del diritto interno, con l'obiettivo di bilanciare l'accesso del pubblico ai documenti ufficiali con il diritto alla protezione dei dati personali.

La normativa specifica per l'accesso a documenti amministrativi che contengono dati personali è delineata nell'articolo 59 del Decreto Legislativo 196/2003. Questo articolo stabilisce che, fatta eccezione per i dati relativi allo stato di salute e alla vita sessuale, le modalità e i limiti per l'esercizio del diritto di accesso, così come la tutela giurisdizionale, sono regolati dalla Legge 241/1990 e dalle altre disposizioni in materia. Questo include anche le categorie particolari di dati e i dati relativi a condanne penali e reati, nonché le operazioni di trattamento possibili.

Se invece l'accesso (documentale) riguarda dati inerenti allo stato di salute ovvero la vita o l'orientamento sessuale o, ancora, dati genetici, l'art. 60 del Codice privacy, con formulazione analoga a quella già vigente, impone di applicare il criterio del bilanciamento di interessi. Il trattamento è infatti consentito soltanto se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso sia di rango almeno pari ai diritti dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale.

Infine, è importante sottolineare che anche nell'ambito delle istanze di accesso si applicano i principi generali del GDPR, in

particolare il principio di minimizzazione. Questo significa che i dati personali devono essere sempre “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati”.

# 10 Rafforzamento delle misure di prevenzione dei data breach

## 10.1 La formazione

La formazione dei dipendenti è un elemento cruciale nella strategia di difesa contro gli attacchi informatici e, in particolare, contro quelli più insidiosi di ingegneria sociale. Questi attacchi, che sfruttano le vulnerabilità umane piuttosto che le debolezze tecniche, possono essere efficacemente contrastati attraverso l'educazione e la sensibilizzazione del personale. Esistono specifici settori della formazione sui quali ciascun ente dovrebbe concentrare la propria attenzione. La formazione, da questo punto di vista, se condotta da esperti nel settore di chiara fama, è una misura in grado di ridurre – pur senza eliminarlo – il rischio di attacchi di quest’ambito:

- **Consapevolezza sui Rischi**: La formazione aiuta i dipendenti a comprendere la natura e le tecniche degli attacchi di ingegneria sociale, come il phishing, il vishing (phishing telefonico), il pretexting o il baiting (esca). La consapevolezza di tali tattiche è il primo passo per la prevenzione, anche con specifico riferimento alla necessità di evitare che i dipendenti forniscano credenziali di autenticazione o altre informazioni particolarmente sensibili.
- **Riconoscimento delle Minacce**: Attraverso esempi pratici e simulazioni, i dipendenti possono imparare a identificare i segni di un tentativo di ingegneria sociale. Ciò include il riconoscimento di email sospette, richieste di informazioni insolite o urgenti e tentativi di manipolazione emotiva.
- **Procedure di Sicurezza**: La formazione fornisce ai dipendenti le conoscenze sulle procedure di sicurezza da seguire in caso di sospetto attacco di ingegneria sociale. Questo include a chi segnalare l'incidente, come gestire le comunicazioni sospette e le misure da adottare per proteggere le informazioni sensibili.

- **Cultura della Sicurezza**: Un programma di formazione continuo contribuisce a creare una cultura dei dipendenti orientata alla sicurezza, dove i dipendenti si sentono responsabili della protezione dei dati e delle risorse dell'ente.
- **Aggiornamento Continuo**: Gli attacchi di ingegneria sociale si evolvono costantemente. La formazione regolare assicura che i dipendenti siano aggiornati sulle ultime tattiche e tecniche utilizzate dagli attaccanti.
- **Rafforzamento delle Competenze**: La formazione aiuta a sviluppare competenze pratiche, come la verifica sicura delle identità nei contatti elettronici e telefonici, e l'uso corretto dei protocolli di sicurezza IT.
- **Riduzione degli Errori Umani**: Molti attacchi di ingegneria sociale sfruttano errori umani. Formare i dipendenti su come evitare comportamenti rischiosi può ridurre significativamente la probabilità di successo di tali attacchi.

In conclusione, la formazione dei dipendenti è essenziale per costruire una linea di difesa umana forte contro gli attacchi di ingegneria sociale, complementare alle misure tecniche di sicurezza.

## 10.2 Il codice di comportamento e i profili di sicurezza

Con il DPR 13 giugno 2023 n. 81 è stato modificato il DPR 16 aprile 2013 n. 62 recante "codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165". In particolare, il DPR 81/2023 ha introdotto gli artt. 11-bis e 11-ter del Codice di comportamento. Secondo il primo comma dell'art. 11-bis, "*l'amministrazione, attraverso i propri responsabili di struttura, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali. In caso di uso di dispositivi elettronici personali, trova*

*applicazione l'articolo 12, comma 3-bis del decreto legislativo 7 marzo 2005, n. 82*". Tale comma evidenzia l'importanza della sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. A contrasto delle eventuali violazioni informatiche vengono introdotte norme specifiche, quindi, che prevedono una responsabilità di tipo disciplinare. Tuttavia, le modalità di tali accertamenti non sono ancora state pubblicate dall'AgID. Si evidenzia, inoltre, che è necessario applicare le norme del Codice dell'Amministrazione Digitale sui dispositivi BYOD, in base alle quali le Amministrazioni "favoriscono l'uso da parte dei lavoratori di dispositivi elettronici personali o, se di proprietà dei predetti, personalizzabili, al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo". Si pensi, ad esempio, ai lavoratori che necessitino, per lo svolgimento dell'attività lavorativa, di dispositivi assistivi (si veda L. 4/2004). Nonostante sia favorito l'uso dei BYOD quando necessari ai lavoratori per lo svolgimento delle proprie mansioni lavorative, la norma in questione evidenzia, comunque, la necessità che sia assicurato, da un lato, la sicurezza per i sistemi informativi dell'ente e, dall'altro, la protezione dei dati personali.

Il secondo comma, dell'art. 11-bis del Codice di comportamento nazionale prevede, inoltre, che l'uso degli account istituzionali sia "consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione" e che anche l'utilizzo delle caselle di posta elettronica personali debba essere evitato per lo svolgimento delle mansioni lavorative "salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale". Da un lato il richiamo alla necessità di utilizzo degli account istituzionali vuole evitare che il lavoratore, mediante un uso distorto degli strumenti messi a disposizione dall'amministrazione per lo svolgimento dell'attività lavorativa possa andare a incidere sulla sicurezza o la reputazione dell'amministrazione e, dall'altro, si vuole evitare che, utilizzando account e strumenti informatici, il lavoratore possa commettere il

reato di accesso abusivo a sistema informatico. Si evidenzia, in sostanza, che gli strumenti lavorativi possano essere impiegati solo per lo svolgimento delle mansioni lavorative e non, ad esempio, per soddisfare una curiosità personale del dipendente o altre finalità estranee a quelle lavorative. Anche l'uso degli account email personali del dipendente è scoraggiato, per finalità lavorative, salvo casi particolari.

## 10.3 Le attività di auditing

In tutte le attività di gestione del rischio – ivi compreso quello che incida sul trattamento dei dati personali o sulla sicurezza dei sistemi informativi – è essenziale (richiamando quelle che sono le attività del ciclo di Deming – PDCA) una corretta attività di auditing il cui scopo è quello di verificare quale sia lo stato delle cose e cosa possa essere fatto per migliorare le attività finalizzate a ridurre il rischio. Oltre che nella fase di primo assessment del rischio, l'auditing è fondamentale in ogni aggiornamento o, se vogliamo, alla riproposizione della fase "check" del ciclo PDCA. Con riferimento alla necessità di garantire sicurezza e integrità delle informazioni, le attività di auditing possono consistere nella:

- **Identificazione dei rischi**: la gestione del rischio inizia sempre con l'identificazione dei potenziali rischi per la sicurezza. Con gli audit si individuano e identificano i rischi, se ne valuta la probabilità e la gravità e, infine, la capacità dell'ecosistema (contesto interno, esterno, normativa applicabile, tipologie di mansioni lavorative, strumenti impiegati etc) di affrontare e resistere all'impatto del rischio ipotizzato.
- **Valutazione delle priorità**: gli audit aiutano a quantificare l'impatto e la probabilità dei rischi, consentendo all'ente di decidere dove concentrare le risorse e gli sforzi di mitigazione.

Una volta eseguito l'auditing iniziale, sarà necessario – sul versante della sicurezza informatica – concentrarsi su alcuni aspetti fondamentali:

- **Valutazione delle politiche di sicurezza (“policy ICT”)**: potrebbe essere necessario, nel caso in cui l’ente si sia dotato di un disciplinare interno sull’uso degli strumenti e degli account istituzionali, revisionarli a cadenze regolari per renderle sempre aggiornate e in linea con le norme in materia di sicurezza;
- **Analisi costante dei rischi**: Si è già detto del rilievo che una costante e attenta attività di auditing ricopre nell’ottica del miglioramento continuo e nel perseguimento della riduzione del rischio;
- **Audit dei sistemi e delle reti**: gli auditing su sistemi e reti servono a rilevare eventuali anomalie, vulnerabilità o attività sospette che potrebbero indicare tentativi di intrusione o altre minacce alla sicurezza;
- **Controllo degli accessi e degli account legittimati**: è fondamentale verificare che le politiche e le procedure di controllo degli accessi siano adeguatamente implementate per prevenire accessi non autorizzati ai dati e alle risorse informatiche. Questi controlli sono utili anche per individuare gli account non più attuali che debbano essere disattivati, come quelli, ad esempio, degli ex-dipendenti;
- **Audit delle procedure di backup e di recupero**: è importante valutare anche l'efficacia e l'affidabilità delle procedure di backup e di recupero dati per garantire la continuità operativa in caso di incidenti. Delle modifiche potrebbero risultare necessarie quando, ad esempio, l’hardware di backup sia obsoleto o non più pienamente funzionante, quando il software non sia più aggiornato rispetto agli update e patch di sicurezza, quando i sistemi di memorizzazione delle informazioni non siano più in grado di assicurare una corretta memorizzazione, quando le condizioni di sicurezza fisica dei dispositivi di backup non sia più assicurata etc.;
- **Formazione e consapevolezza del personale**: si è già detto dell’importanza di una approfondita e costante formazione dei dipendenti sui profili di sicurezza informatica e protezione dei dati personali;
- **Revisione dei contratti con terzi**: una importanza appropriata deve essere attribuita non soltanto alla scelta dei soggetti ai quali affidare il trattamento di dati personali o la gestione anche solo di parte delle politiche di sicurezza dell’ente. Oltre al momento di individuazione del terzo, in cui si dovrà verificare l’affidabilità e la

capacità di attuare le politiche di sicurezza corrette, sarà necessario anche porre un'attenzione particolare alle specifiche clausole che regolano i rapporti con i soggetti terzi. Si pensi, ad esempio, all'importanza delle clausole ex art. 28 GDPR sulla nomina del responsabile del trattamento (che, come noto, è sempre un soggetto esterno all'organizzazione del titolare del trattamento);

- **PenTesting**: nonostante si tratti di attività pressoché sconosciute agli enti pubblici occorre rilevare che i test di penetrazione, quando condotti da professionisti qualificati, hanno un enorme impatto positivo in relazione alla sicurezza dei sistemi informativi dell'ente. Il pentesting è, in sostanza, un'attività contrattualizzata con la quale i professionisti in questione simulano attacchi informatici e testano la resilienza dei sistemi. All'esito delle attività di pentesting, l'ente ottiene dagli auditor un report sulle azioni da intraprendere per compensare le debolezze individuate e rafforzare (hardening) la capacità di risposta;
- **Audit dei registri e dei log di sistema**: benché si tratti di attività riservate a personale esperto, l'analisi dei file di log è essenziale per rilevare anomalie o attività sospette. Si potrebbero, allo scopo, anche predisporre software di analisi (come, ad esempio, IDS o IPS, ossia intrusion detection system e intrusion prevention system) finalizzati a prevenire e rilevare eventuali tentativi di intrusione nei sistemi informativi dell'ente.

# Gestione del data breach

La violazione dei dati personali è definita, come già accennato in precedenza, dall'art. 4 comma 12 del GDPR come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". Si tratta, per l'appunto, di una violazione di sicurezza o "data breach".

L'art. 29 WP (Gruppo dell'articolo 29 per la tutela dei dati - Article 29 Working Party), nelle proprie linee guida sulle violazioni di dati personali, distingue tre categorie, basandosi sui principi di sicurezza delle informazioni:

- ☑ Violazioni della **confidenzialità**: si verifica ad esempio quando un errore del sistema consente anche a terzi non autorizzati di accedere ai dati personali;
- ☑ Violazioni dell'**integrità**: consiste in una accidentale o non autorizzata alterazione dei dati;
- ☑ Violazione della **disponibilità**: si riscontra ad esempio quando l'azione di un ransomware (un software malevolo che opera cifrando i dati dei sistemi, per richiedere poi un riscatto) provochi la perdita dell'accesso o la distruzione dei dati personali.

Naturalmente, una violazione può rientrare in più categorie contemporaneamente. Si pensi all'azione di chi si introduce indebitamente nel sistema, prenda visione di dati personali e li alteri, comportando una violazione sia di confidenzialità che di integrità. O al caso in cui venga smarrito un supporto che contiene dati personali e non se ne abbia una copia (violazione di confidenzialità e di disponibilità).

## 11 Sicurezza informatica e possibilità di prevedere le violazioni

Il GDPR, in coerenza al principio di responsabilizzazione e di sicurezza, impone l'adozione di un sistema di misure tecniche e organizzative adeguate a prevenire (anche) le violazioni di dati personali.

Le misure di sicurezza, come precedentemente esaminate, devono includere sistemi per la rilevazione delle violazioni. Questi sistemi devono essere integrati in modo organico con le misure organizzative per la gestione delle violazioni, e tali procedure devono essere rese note anche ai soggetti esterni all'ente, come ad esempio i responsabili del trattamento dei dati personali, come definiti dall'articolo 28 del GDPR, e alle società incaricate della manutenzione dei sistemi informatici.

Nel gestire le violazioni, oltre ai profili formali, è essenziale adottare misure appropriate per risolvere le violazioni stesse. Infatti, la minimizzazione dei possibili danni rappresenta uno degli obblighi principali del titolare del trattamento dei dati.

## 12 Documentazione del data breach: il registro delle violazioni

In linea con il principio di responsabilizzazione stabilito dal GDPR, è fondamentale che le organizzazioni adottino procedure specifiche per la gestione delle violazioni di dati personali. Queste procedure devono chiaramente definire i soggetti coinvolti nel processo e delineare i passaggi chiave da seguire, fino all'eventuale notificazione all'Autorità Garante per la protezione dei dati personali, o alla comunicazione agli interessati in caso di violazione.

L'implementazione di uno strumento specifico, come ad esempio un vademecum, per la gestione delle violazioni di dati personali ha l'obiettivo di sistematizzare e rendere più efficiente la risposta ai data breach. Questo comporta l'identificazione dei soggetti coinvolti nella

gestione operativa delle violazioni e la definizione di un insieme standard di attività da intraprendere per mitigare e riparare il danno causato dalla violazione. Tale approccio non solo assicura la conformità con le normative vigenti, ma aumenta anche l'efficacia nell'affrontare e limitare gli impatti negativi dei data breach.

È bene ricordare che il GDPR all'art. 33, comma 5, impone di documentare qualsiasi violazione (con l'indicazione delle circostanze, delle conseguenze e dei successivi provvedimenti adottati).

## 13 Notifica all'Autorità di Controllo

Il GDPR stabilisce l'obbligo per i titolari del trattamento di notificare le violazioni di dati personali (i cosiddetti 'data breach') all'Autorità di controllo nazionale, in Italia rappresentata dal Garante per la Protezione dei Dati Personali. La notifica al Garante deve avvenire entro 72 ore dalla scoperta dell'incidente da parte del titolare, non dal momento in cui l'incidente si è verificato. Questo termine inizia a decorrere dal momento in cui il titolare acquisisce una 'ragionevole certezza' che un incidente di sicurezza abbia effettivamente compromesso dei dati personali. In caso di ritardi nella notifica, è necessario fornire una motivazione valida per il ritardo.

La notifica è obbligatoria a meno che non sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Una valutazione, anche sommaria, del rischio è dunque richiesta per determinare l'obbligatorietà della notifica. Ad esempio, può essere considerata 'improbabile' la necessità di una notifica in casi come l'incidente che coinvolge dati già resi pubblici, come quelli pubblicati nella sezione 'Amministrazione Trasparente', o in situazioni di indisponibilità transitoria dei dati che non hanno impatti significativi, come in caso di un blocco temporaneo di sistemi informatici.

Ulteriori esempi e linee guida sull'interpretazione e l'applicazione di queste regole possono essere trovati nelle Linee-guida 01/2021 del Comitato Europeo per la Protezione dei Dati personali (EDPB). Tra i

rischi menzionati dalle Linee guida EDPB 01/2021, che possono avere rilevanza, troviamo:

- Data breach causato da un attacco ransomware
    - Con backup delle informazioni disponibile e senza esfiltrazione dei dati
    - Senza preventivo backup
    - Senza backup e con esfiltrazione dei dati
- Data breach causato da un attacco finalizzato all'esfiltrazione dei dati
    - Esfiltrazione dal sito web
    - Esfiltrazione delle credenziali di autenticazione dal sito web
- Data breach causato da un dipendente
    - Esfiltrazione di informazioni da parte di un dipendente o ex dipendente
    - Trasmissione accidentale di informazioni a terze parti fidate
- Perdita o furto di dispositivi e documenti cartacei
    - Furto di dispositivi di archiviazione contenenti dati cifrati.

L'art. 33 comma 3 del GDPR indica il contenuto minimo della notifica:

- La descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- Il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro soggetto presso cui ottenere più informazioni;
- La descrizione delle probabili conseguenze delle violazioni dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e per attenuare i possibili effetti negativi.

L'articolo 33, comma 3, del GDPR specifica in dettaglio il contenuto minimo che deve essere incluso in una notifica di violazione dei dati personali. Questo include:

- **Descrizione della violazione**: Una descrizione dettagliata della natura della violazione dei dati personali. Ciò include, ove possibile,

indicare le categorie e il numero approssimativo di soggetti interessati (persone fisiche i cui dati sono stati compromessi) e le categorie e il numero approssimativo di registrazioni dei dati personali coinvolti.

- **Contatti del Responsabile della Protezione dei Dati (DPO)**: Deve essere fornito il nome e i dati di contatto del DPO, se nominato, o di un altro soggetto che può fornire ulteriori informazioni riguardo alla violazione. Questo facilita le comunicazioni e fornisce un punto di riferimento per ulteriori domande o chiarimenti.
- **Conseguenze e misure correttive**: Deve essere inclusa una descrizione delle probabili conseguenze della violazione dei dati personali. Inoltre, è necessario descrivere le misure che sono state già adottate o che si propone di adottare per porre rimedio alla violazione e per mitigare i possibili effetti negativi. Questo potrebbe includere azioni intraprese per limitare i danni o per prevenire future violazioni.

Queste informazioni sono essenziali per consentire all'Autorità Garante per la Protezione dei Dati Personali di comprendere la portata e la gravità della violazione e per valutare l'adeguatezza della risposta dell'organizzazione. La comunicazione dei data breach all’autorità Garante per la protezione dei dati personali viene fatta attraverso una pagina specifica messa a disposizione dei titolari del trattamento dei dati personali sul sito web dell’Autorità.

## 14 Ipotesi di comunicazione agli interessati

L’art. 34 del GDPR impone l’obbligo per il titolare, accanto alla notifica al Garante, di comunicare agli interessati la violazione di dati personali, laddove questa possa provocare un rischio elevato per i diritti e le libertà delle persone fisiche. In alcuni casi, anche il Garante può richiedere che questa comunicazione venga effettuata se ravvisa un rischio elevato per i dati personali.

La comunicazione agli interessati deve avvenire il più presto possibile e senza ingiustificato ritardo. È importante che la comunicazione sia redatta in un linguaggio semplice e chiaro, e deve

descrivere gli elementi indicati nell'articolo 33 del GDPR, quali la natura della violazione, i possibili effetti e le misure adottate o proposte per affrontare la violazione.

Tuttavia, l'articolo 34, comma 3, del GDPR prevede alcune eccezioni a questo obbligo di comunicazione:

- **Misure tecniche e organizzative**: Se il titolare ha implementato misure tecniche e organizzative adeguate che proteggono i dati coinvolti nella violazione, specialmente misure che rendono i dati incomprensibili a chiunque non sia autorizzato, come la cifratura.
- **Misure adottate successivamente al data breach**: Se il titolare ha adottato misure dopo la violazione che eliminano il rischio elevato per i diritti e le libertà degli interessati.
- **Sforzi sproporzionati per la comunicazione individuale**: Se la comunicazione individuale ad ogni interessato richiederebbe sforzi sproporzionati. In questi casi, il titolare può ricorrere a metodi alternativi, come comunicazioni pubbliche o simili, per informare gli interessati.

In conclusione, mentre il GDPR impone la comunicazione diretta agli interessati in caso di violazioni che presentano un rischio elevato, prevede anche alcune eccezioni importanti per mitigare il carico amministrativo sui titolari del trattamento, sempre nel rispetto dei diritti degli interessati.

## 15 Il ripristino dei dati in caso di incidente

Uno degli aspetti fondamentali nella gestione della sicurezza e della privacy è la capacità del titolare del trattamento di assicurare continuamente la tutela dei dati personali. Questa tutela comprende diverse componenti chiave: la riservatezza, l'integrità, la disponibilità e la resilienza dei dati.

Per raggiungere questo obiettivo, è essenziale implementare un sistema che permetta il ripristino tempestivo delle informazioni in caso di incidenti informatici o altre interruzioni. Come precedentemente sottolineato nell'ambito dell'obbligo di sicurezza e

nel contesto della Misura Minime di Sicurezza per la Pubblica Amministrazione (MMS-PA – individuate dalla circolare AgID 2/2017), la capacità di recuperare rapidamente i dati dopo un incidente è un elemento vitale per garantire la continuità operativa e la protezione dei dati.

Questo implica l'adozione di strategie e strumenti efficaci, come:

- **Backup regolari**: Mantenere backup regolari dei dati, sia in siti fisici che in cloud, per garantire che possano essere recuperati in caso di perdita.
- **Piani di ripristino di emergenza**: Sviluppare e testare piani di ripristino di emergenza che descrivano le procedure da seguire in caso di incidenti di sicurezza o malfunzionamenti tecnici.
- **Ridondanza dei dati**: Implementare sistemi di ridondanza per assicurare che i dati critici siano duplicati e possano essere accessibili anche in caso di guasti hardware o software.
- **Formazione del personale**: Assicurare che il personale sia adeguatamente formato per riconoscere e reagire prontamente agli incidenti di sicurezza, minimizzando così i tempi di inattività e il potenziale danno.
- **Test e valutazione continui**: Eseguire regolarmente test e valutazioni per assicurare che i sistemi di backup e ripristino siano sempre efficienti e aggiornati.

In conclusione, garantire la resilienza e la capacità di ripristino dei dati personali è un impegno continuo che richiede un'attenta pianificazione, implementazione di misure tecniche adeguate e formazione continua del personale. Questo approccio consente di proteggere i dati personali contro una vasta gamma di rischi, assicurando al tempo stesso la conformità alle normative vigenti in materia di sicurezza e privacy.

## 16 La segnalazione del data breach ai sensi della circolare AgID 2/2017

Come già visto in precedenza, la Circolare AgID n. 2/2017, rubricata “Misure minime di sicurezza ICT per le pubbliche amministrazioni”,

prescrive alle PA (a tutte le Amministrazioni di cui all'art. 2, comma 2, del D. Lgs. 82/2005) di comunicare le violazioni di sicurezza anche al CERT-PA.

L'art. 4 della Circolare 2/2017 dell'AgID prevede che il modulo di implementazione sia firmato digitalmente con marcatura temporale. Dopo la sottoscrizione il modulo di implementazione delle MMS-PA "*deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso*".

# 17 Monitoraggio e aggiornamento

L'ultima fase nel processo di gestione del rischio consiste nel monitoraggio costante delle misure proattive adottate, nella verifica della loro efficacia e, se necessario, nell'aggiornamento sia del processo di valutazione del rischio sia delle contromisure più appropriate. È fondamentale riconoscere che la gestione del rischio non è un prodotto finito o un punto d'arrivo definitivo. Piuttosto, la sicurezza informatica e le misure tecniche e organizzative per la riduzione del rischio sono processi in continua evoluzione che richiedono un monitoraggio e un adeguamento costanti. Questa realtà è ben sintetizzata dall'acronimo PDCA (Plan, Do, Check, Act), noto anche come 'Ciclo di Deming', che enfatizza un approccio continuo al miglioramento nella gestione della qualità, in questo caso specifico, nella gestione del rischio associato alla protezione dei dati personali.

Nelle discipline di sicurezza e privacy che abbiamo esaminato, sono state identificate diverse figure chiave, come il Data Protection Officer (DPO) previsto dal GDPR, il Responsabile per la Prevenzione della Corruzione e della Trasparenza (RPCT) secondo la legge 190/2012, l'Organismo di Vigilanza (OdV) del decreto legislativo 231/2001, e il Responsabile del Servizio di Prevenzione e Protezione (RSPP) del decreto legislativo 81/2008. La caratteristica comune e fondamentale di queste figure è l'autonomia e l'indipendenza nello svolgimento delle loro funzioni, essenziali per garantire che le attività di monitoraggio e controllo siano libere da interferenze interne all'ente. Questa

autonomia è talmente cruciale che, in assenza di indipendenza dal vertice dell'ente, la loro efficacia può essere compromessa, con conseguenze significative in termini di conformità normativa.

Queste figure — DPO, RPCT, OdV e RSPP — rappresentano dunque un ulteriore baluardo nella gestione e nel contrasto dei rischi, grazie alla loro capacità di operare in modo autonomo e indipendente, anche nel contesto del monitoraggio e della revisione delle pratiche di sicurezza. Data la natura complementare di queste figure, è essenziale che tra loro, o tra figure analoghe individuate dall'ente, vi sia un costante scambio di informazioni. Questa collaborazione aiuta a prevenire la creazione di 'camere stagne' in cui le informazioni sui rischi vengono isolate in silos separati e non comunicanti. Una comunicazione aperta e regolare tra queste figure chiave consente un approccio più efficiente, accurato e tempestivo nella risposta agli eventi rilevanti, massimizzando così l'efficacia delle strategie di prevenzione e mitigazione dei rischi. In definitiva, la cooperazione e la condivisione delle informazioni tra DPO, RPCT, OdV e RSPP sono fondamentali per garantire una visione olistica della gestione del rischio e per implementare un sistema di sicurezza più robusto e reattivo, in grado di affrontare efficacemente una varietà di sfide in ambito di sicurezza e privacy.