19 Settembre 2025

L’integrità dei dati, una declinazione della loro qualità

Di Giovanni Fiorino

Abstract

Il contributo si propone di esaminare l’incidenza delle politiche di sicurezza informatica sull’attività di formazione delle risorse umane. In particolare, esso prende le mosse dallo studio dei report delle minacce informatiche di CLUSIT e dell’Agenzia per la cybersicurezza nazionale, entrambi aggiornati al 2024, nonché dalla constatazione che le vulnerabilità principali riguardano il c.d. “fattore umano”, da sempre identificato come il vero anello debole della catena della sicurezza informatica. In tale prospettiva, vengono esaminate le disposizioni normative contenute sia nel Regolamento europeo n. 679/2016 (GDPR) che nel Decreto legislativo n. 138/2024 e nella Legge n. 90/2024, che si occupano della cybersicurezza nazionale: il filo conduttore degli impianti normativi è rappresentato dalla importanza delle linee guida – di ENISA e dell’Agenzia per la cybersicurezza nazionale – nella individuazione delle misure di sicurezza necessarie perché, anche nell’ottica dell’accountability, possano considerarsi adempiuti gli obblighi gravanti, a vario titolo, sui destinatari nelle norme che impongono la sicurezza dei dati e dei sistemi che li contengono. In ossequio al tema del contributo, l’analisi delle linee guida ha riguardato le misure finalizzate alla formazione delle risorse umane.

Indice

Introduzione

La **cybersecurity** comprende l’insieme di attività, tecniche e strumenti volto a garantire **la riservatezza, l’integrità e la disponibilità dei dati e dei sistemi informatici**[1]. Essa passa necessariamente attraverso un vero e proprio processo che va a coinvolgere tutte le componenti di un sistema informatico: **hardware, software e humanware**.

Da un punto di vista strettamente giuridico, la cybersecurity è sempre stata vista sia come un obbligo connesso al trattamento dei dati sia come un elemento indispensabile di alcune fattispecie penalistiche, al fine di constatare l’abusività dell’azione commessa contro sistemi informatici o dati in essi contenuti[2].

La definizione di cybersecurity pone subito in evidenza due aspetti: il primo attiene all'**oggetto della sicurezza**, che si identifica non soltanto nei **"dati"** ma anche nei **"sistemi informatici"** che li contengono. Il secondo riguarda la procedimentalizzazione della cybersecurity che coinvolge hardware, software ed humanware, termine informatico utilizzato per definire le risorse umane di un sistema informatico o l'hardware e il software progettati tenendo conto dell'esperienza e dell'interfaccia dell'utente finale[3].

> In questo quadro, il fattore umano rappresenta un elemento fondamentale della sicurezza e, al tempo stesso, può costituire una vulnerabilità che si confronta con una modalità di intrusione non tecnica nota come **"social engineering"**: essa si basa sull'interazione umana e, spesso, c**omporta l'inganno di altre persone, sfruttando le "debolezze" umane e le falle presenti nelle procedure di sicurezza**.

Questo tipo di attacco si rivela spesso molto efficace perché è mirato al punto più debole della catena della sicurezza informatica (solitamente l'essere umano) e si basa sul fatto che molte persone non sono ancora abituate a gestire l'informazione di una società che si fonda intensamente sulla *communication tecnology*, inconsapevoli del valore dei dati e non preoccupati di proteggerli[4].

Minacce informatiche e fattore umano nel Rapporto CLUSIT 2024 e nella Relazione annuale al Parlamento, per il 2024, dell'Agenzia per la cybersicurezza nazionale

Prima di esaminare le questioni tecniche e giuridiche connesse alla sicurezza dei dati e dei sistemi informatici, è necessario conoscere la tipologia delle minacce informatiche attraverso i documenti costituiti dal rapporto CLUSIT e dalla relazione annuale dell'Agenzia per la cybersicurezza nazionale, entrambi aggiornati al 2024.

L'esame del rapporto CLUSIT 2024, sulla sicurezza ICT in Italia[5], conferma **il dominio del malware** [6] tra gli attacchi informatici e rileva **la costante gravità "degli incidenti basati su tecniche di *Phishing / Social Engineering (20%)*, DdoS (quasi 20%) e *Identity Theft / Account Cracking* (di poco superiore al 20%)"**: in particolare, lo studio della cybersecurity nelle piccole e medie imprese[7] rileva che "nelle aziende piccole e piccolissime (fino a 10 collaboratori) si arriva ad un 80% che non dispone di personale dedicato all'informatica, e si appoggia pesantemente a fornitori esterni", mentre spesso "(nel 64% delle microimprese) si tratta di una persona sola, proveniente da un fornitore, alla quale vengono richiesti anche compiti di cybersecurity".

> Secondo il rapporto, "la formazione rimane comunque un ambito con cui le aziende faticano a confrontarsi" ed è particolarmente significativo "il dato che anche nelle aziende più grandi del campione solo poco più di metà offre ai collaboratori una formazione sia in ambito cybersecurity sia privacy, e solo circa 1/3 lo fa in modo regolare. Per le microimprese, il dato è desolante: per 9 realtà su 10 la formazione è del tutto assente".

A parere dell'associazione, "per migliorare la postura di cybersecurity delle aziende sembra consigliabile investire nella formazione dei collaboratori e nell'adozione di politiche formalizzate. In particolare, **è importante creare un ambiente in cui le aziende possano condividere esperienze e conoscenze relative alla gestione della cybersecurity**, in modo da poter raggiungere una maggiore consapevolezza dei rischi e delle opportunità di protezione, così come raccomandato dalle migliori pratiche e dalla legislazione in vigore"[8].

Quanto sopra è sovrapponibile alle indicazioni contenute nella Relazione annuale al Parlamento dell'Agenzia per la cybersicurezza nazionale per il 2024[9]: in particolare, nella stessa è scritto che "affinché un attore ostile possa compromettere sistemi, account o applicazioni è necessario che riesca a ottenere l'accesso all'interno di una rete o di un sistema informatico. Per raggiungere tale obiettivo **vengono sfruttati specifici vettori di attacco che consentono all'attaccante di eludere le misure di sicurezza ed esercitare un controllo non autorizzato sulla rete o sul sistema informatico**. Tali vettori possono essere impiegati non solo per ottenere un accesso iniziale, ma anche per consolidare la presenza all'interno dell'ambiente compromesso o per evitare il rilevamento".

I **"vettori di attacco"** vengono individuati, tra gli altri: **nella email**, attraverso l'impiego "di comunicazioni fraudolente per indurre l'utente a divulgare credenziali, eseguire codice malevolo o fornire informazioni sensibili"; **negli account validi**, attraverso lo sfruttamento di "credenziali compromesse, ottenute tramite esfiltrazione di dati, attacchi di forza bruta o *phishing*, per accedere ai sistemi con identità legittime, riducendo le probabilità di rilevamento e favorendo il movimento laterale"; **nei social media**, attraverso la "diffusione di contenuti ingannevoli per raccogliere informazioni sensibili o agevolare ulteriori fasi dell'attacco informatico, come la profilazione di specifici bersagli per operazioni mirate".

Sul punto, nella Relazione è scritto che: "La preponderanza dell'impiego dell'e-mail quale vettore per l'inizio della maggior parte degli attacchi richiama l'importanza cruciale che riveste il fattore umano quale argine determinante contro le minacce cyber"[10].

> **Minacce informatiche e vulnerabilità sono i due poli all'interno dei quali si gioca la partita della sicurezza**, ovvero della protezione della integrità dei dati e dei processi di trattamento degli stessi: tale esigenza, già presente nel Regolamento europeo n. 679/2016 (GDPR), è stata ulteriormente disciplinata sia mediante il decreto legislativo n. 138/2024, di attuazione della Direttiva del Parlamento europeo n. 2022/2555 (c.d. NIS2) sia mediante la legge n. 90/2024 contenente anche "Disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario".

L'integrità dei dati e la sicurezza dei processi di trattamento nel regolamento europeo n. 679/2016 (GDPR): le linee guida ENISA e l'attività di formazione del personale

A norma dell'articolo 5 comma 1 lettera f) del Regolamento (UE) 2016/679, i dati personali sono trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza») mediante "misure tecniche e organizzative adeguate".

In particolare, l'articolo 32, rubricato **"Sicurezza del trattamento"**, fornisce un'indicazione non esaustiva delle "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" stabilendo che esse comprendono, tra le altre, "la pseudonomizzazione e la cifratura dei dati personali", "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico" e "la capacità d assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento".

Il quadro normativo di riferimento è completato dal principio di ***accountability***, da intendersi quale **l'adozione, da parte del titolare del trattamento dei dati, di comportamenti proattivi atti a dimostrare la conformità del trattamento dei dati personali ai principi del regolamento**[11].

> A fronte della tipizzazione, da parte del legislatore europeo, di sole due misure di sicurezza tecniche, la pseudonimizzazione e la crittografia, è necessario ricorrere a linee guida e standard internazionali al fine di individuare ulteriori specifiche misure di sicurezza da adottare – previa la valutazione del rischio per i diritti e le libertà degli interessati.

In tale prospettiva, assumono particolare rilievo le **"Technical guidelines for the implementation of minimum security measures for Digital Service Providers"** dell'European Union Agency for Network and Information Security, redatte da ENISA, ossia l'Agenzia europea per la sicurezza informatica[12].

L'analisi delle Linee guida[13]consente di individuare l'obiettivo riguardante la gestione del personale sia in termini di conoscenze sia in termini di verifica dell'esperienza e dell'affidabilità dei dipendenti interni all'organizzazione: in particolare, assume rilievo il sesto obiettivo, "Security knowledge and training" così descritto: "Il DSP verifica e garantisce che il personale abbia una conoscenza sufficiente della sicurezza e che riceva una formazione regolare in materia di sicurezza. Ciò si ottiene, ad esempio, attraverso attività di sensibilizzazione, educazione alla sicurezza, formazione sulla sicurezza, ecc.".

Le misure di sicurezza relative alla formazione delle risorse umane sono individuate in gruppi di tre livelli, con indicazione dei relativi esempi: quelle del **primo livello** sono finalizzate a "fornire regolarmente al personale chiave formazione e materiale pertinente sulle questioni di sicurezza", nonché a "garantire che le terze parti siano formate e consapevoli delle problematiche di sicurezza", in entrambi i casi rileva lo strumento del colloquio.

Le misure di sicurezza del **secondo livello** sono così individuate: "Implementare un programma di formazione [che dev'essere approvato dalla direzione] assicurandosi che il personale chiave abbia conoscenze di sicurezza sufficienti e aggiornate" ed "organizzare corsi di formazione e sessioni di sensibilizzazione per il personale su argomenti di sicurezza importanti per l'organizzazione".

Le misure di sicurezza del **terzo livello** si occupano delle modalità inerenti la formazione del personale stabilendo, in primo luogo, che "i contenuti della formazione sulla sicurezza si basano sui ruoli e sulle responsabilità assegnati e sui requisiti specifici dell'organizzazione e del sistema informativo a cui il personale ha accesso autorizzato" e che il programma di formazione sia rivisto ed aggiornato periodicamente, "tenendo conto dei cambiamenti e degli incidenti passati".

Le linee guida, inoltre, prevedono che vengano stabiliti "contatti e canali di comunicazione con gruppi e associazioni di sicurezza per rimanere aggiornati sulle più recenti pratiche, tecniche e tecnologie di sicurezza raccomandate" e che al personale siano offerte "sessioni di formazione per ottenere certificazioni di sicurezza riconosciute".

> Nell'ottica dell'accountability – da intendersi, per quanto ci occupa, non solo quale scelta responsabile delle modalità di protezione dei dati personali e dei sistemi di trattamento ma anche quale possibilità di dimostrare le scelte operate – **le linee guida** , negli esempi relativi alle misure di sicurezza da adottarsi per perseguire l'obiettivo inerente la formazione del personale, **individuano la predisposizione di verbali delle sessioni di revisione del programma di formazione, dell'elenco dei contatti con gruppi e associazioni di sicurezza, dei risultati dei test sulle conoscenze di sicurezza del personale, dei risultati del processo di certificazione individuale.**

L’evoluzione della cybersicurezza nel decreto legislativo n. 138/2024 e nella legge n. 90/2024

La cybersicurezza è l’oggetto specifico della sopra citata **Direttiva NIS 2,** che ha trovato attuazione, in Italia, con il **decreto legislativo n. 138/2024**, oggi affiancato dalla **legge n. 90/2024** contenente **“Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici”**.

Entrambe le normative fanno riferimento a misure tecniche ed organizzative finalizzate a garantire la sicurezza dei sistemi informativi e di rete.

Nel d.lgs. 138/2024, l’articolo 24 reca: “I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l’impatto degli incidenti per i destinatari dei loro servizi e per altri servizi”.

Inoltre, alla luce della determinazione ACN 164179 del Direttore Generale dell’Agenzia per la cybersicurezza nazionale avente ad oggetto le “Specifiche di base per l’adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS”[14], ACN è chiamata a stabilire “obblighi proporzionati tenuto debitamente conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico”. Quanto sopra è altresì specificato dall’articolo 2 della stessa, secondo cui “In fase di prima applicazione del decreto NIS sono adottate le specifiche di base di cui agli allegati 1, 2, 3 e 4”.

Dunque, anche il decreto legislativo n. 138/2024 rinvia a norme di carattere tecnico, contenute nei ricordati allegati, al fine di individuare le misure tecniche, operative e organizzative necessarie a garantire la sicurezza dei sistemi informativi e di rete: sia l’allegato n. 1 – dedicato alle “Misure di sicurezza di base per i soggetti importanti” – che l’allegato n. 2 – dedicato alle “Misure di sicurezza di base per i soggetti essenziali” – si occupano delle “risorse umane” e delle competenze necessarie a evitare la vulnerabilità dei sistemi rappresentata dall’assenza di formazione[15].

In entrambi gli allegati è previsto che l’individuazione sia del personale autorizzato ad accedere ai sistemi informativi e di rete rilevanti sia degli amministratori di tali sistemi avvenga previa “valutazione dell’esperienza, capacità e affidabilità” e dietro “idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica”.

> L’Agenzia Nazionale per la Cybersicurezza, infine, ha adottato le “Linee guida per il rafforzamento della resilienza dei soggetti di cui all’articolo 1 comma 1 della legge 28 giugno 2024 n. 90”, contenenti misure di sicurezza da applicare ai sistemi informativi e di rete dei soggetti individuati dall’articolo 1 comma 1 della stessa legge[16].

In particolare, **tra le misure di sicurezza, sono elencate quelle attinenti alle risorse umane ed alla formazione degli utenti**, identificate con i codici PR.AT-1 e PR.AT-2, che riguardano, rispettivamente, l’informazione e l’addestramento di tutti gli utenti e la comprensione di ruoli e responsabilità degli utenti con privilegi (ad esempio gli amministratori di sistema).

Entrambe le misure richiedono di prevedere un percorso di formazione per tutti gli utenti e di redigere un documento, che riporti i contenuti delle attività formative effettuate e che descriva le modalità con le quali è verificato l’apprendimento dei contenuti.

Quanto alle modalità di implementazione raccomandate per queste misure, è stabilito che “nel rispetto delle politiche di cybersecurity e nell’ambito del processo di formazione del personale [è necessario] definire un percorso didattico che, a partire dall’analisi del fabbisogno formativo degli utenti, definisca i

contenuti della formazione e ne preveda la verifica dell'apprendimento" nonché "redigere e mantenere aggiornato il registro con l'elenco degli utenti che hanno ricevuto la formazione e i relativi contenuti".

Conclusioni

> La conoscenza della normativa anche tecnica, alla quale rinviano le norme in materia di sicurezza informatica, consente ai soggetti destinatari degli obblighi giuridici di predisporre quanto necessario per garantire l'integrità dei dati e, prima, l'affidabilità dei sistemi informatici che li contengono e che ne consentono il trattamento.

Mediante la predisposizione e la documentazione delle attività di formazione delle risorse umane, sarà possibile evitare, o quantomeno ridurre, la vulnerabilità rappresentata dalla non conoscenza e dalla sottovalutazione del rischio collegato all'utilizzo delle risorse hardware e software, vulnerabilità che rischia di esporre l'intera infrastruttura informatica e telematica, quand'anche ineccepibile dal punto di vista tecnico, a pericolosi attacchi informatici che ne compromettano la funzionalità e determinino, come effetto, un danno per l'integrità dei dati e, dunque, per la qualità degli stessi.

NOTE

[1] In particolare, il Regolamento (UE) 2019/881, più comunemente noto come Cybersecurity Act, all'articolo 2 definisce la «cibersicurezza» come: "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche". Sul piano nazionale, inoltre, il D. Lgs. 138/2024, che ha recepito la Direttiva (UE) 2022/2555 (Direttiva NIS 2), all'articolo 2, lett. q), reca la definizione di «sicurezza dei sistemi informativi e di rete»: "la capacità dei sistemi informativi e di rete di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi. Lo stesso decreto, alla lettera r), definisce la «sicurezza informatica» come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche, così come definito dall'articolo 2, punto 1), del regolamento (UE) 2019/881" (esplicito il rimando al sopracitato Cybersecurity Act). Infine, alla lettera s), è fornita la definizione di «cybersicurezza»: "ferme restando le definizioni di cui alle lettere q) e r), l'insieme delle attività di cui all'articolo 1, comma 1, lettera a), del decreto legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109".

[2] Pierluigi Perri, voce "Cybersecurity" in AAVV, Dizionario Legal tech, a cura di Giovanni Ziccardi e Pierluigi Perri, Milano, 2020, pagg. 268 ss.

[3] "Humanware", consultabile qui (ultima consultazione il 29 luglio 2025).

[4] Giovanni Ziccardi, voce "Social engineering" in AAVV Dizionario Legal tech, loc. cit., pagg. 886 s.

[5] Il Rapporto CLUSIT 2024 fa parte delle pubblicazioni di CLUSIT, Associazione italiana per la sicurezza informatica, ed è scaricabile e consultabile a questo link (ultima consultazione il 29 luglio 2025).

[6] Un software malevolo in grado di interferire con le operazioni svolte su un dispositivo informatico al fine di disturbare l'attività dell'utente, cagionare danni all'utente e/o vantaggi al propagatore e la protezione dal quale richiede un "uso consapevole e attento delle tecnologie". Cfr Luigi Cristiano, voce

“Malware” in AAVV, Dizionario Legal tech, pagg. 611 s.

[7] Rapporto CLUSIT, loc. cit., pagg. 125 ss.

[8] Rapporto CLUSIT, loc. cit. pag. 134.

[9] L’Agenzia per la cybersicurezza nazionale (ACN) è l’Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza. L’Agenzia ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico. La Relazione può essere consultata e scaricata a questo link (ultima consultazione il 29 luglio 2025).

[10] Relazione annuale al Parlamento, loc. cit., pag. 35.

[11] Giulia Escurolle, voce “Accountability” in AAVV, Dizionario Legal tech, op. cit., pagg. 15 ss.

[12] Il sito ufficiale di ENISA si trova al questo link (ultima consultazione il 29 luglio 2025).

Sulla rilevanza delle Linee guida elaborate da ENISA nella prospettiva dell’articolo 32 del regolamento europeo n. 679/2016 cfr. Francesco Capparelli, commento all’articolo 32 del regolamento europeo n. 679/2016 in AAVV, Codice della disciplina privacy, Diretto da Luca Bolognini ed Enrico Pelino, Milano, 2019, pagg. 233 ss.

[13] Le linee guida ENISA sono consultabili e scaricabili al questo link (ultima consultazione il 29 luglio 2025).

[14] La determinazione, ed i relativi allegati, sono consultabili e scaricabili a questo link (ultima consultazione il 29 luglio 2025). In merito a tali documenti l’ACN, nel settembre 2025,ha pubblicato le “Linee guida NIS. Specifiche di base. Guida alla lettura” consultabile a questo link (ultima consultazione il 5 settembre 2025).

[15] In particolare, negli allegati nn. 1 e 2 alla determinazione ACN n. 164179 del 14 aprile 2025 si ritrovano i codici relativi alla formazione del personale (PR.AT-01) ed a quella degli “individui che ricoprono ruoli specializzati” (PR.AT-02).

[16] Le linee guida sono consultabili e scaricabili a questo link (ultima consultazione il 29 luglio 2025).