PRIVACY News®

ANNO 16 | numero 2 | duemila26

CON INFORMATIVE PRIVACY NON TRASPARENTI SI PERDE LA FIDUCIA DEGLI UTENTI E SI RISCHIANO SANZIONI

AUMENTA IL RISCHIO SULLA CYBERSECURITY:

+26% di segnalazioni
e +51% di ransomware

Editore: Associazione Federprivacy – Poste Italiane Spa : Spedizione in abbonamento postale Aut. n. 0434/2021 del 18.02.2021 Stampe periodiche in regime libero – Direttore Responsabile: Nicola Bernardi

BUSTO ARSIZIO MILANO • ROMA

Il nostro studio lo fanno le persone.

Assistiamo le imprese di piccole, medie
e grandi dimensioni di ogni settore

A&A

ALBÈ & ASSOCIATI

STUDIO LEGALE

www.albeeassociati.it | avvocati@albeeassociati.it

EDITORIALE

Negli ultimi tempi la trasformazione digitale ha cambiato in modo radicale la maggior parte dei servizi di cui in passato si usufruiva presso luoghi fisici, e ormai si svolgono prevalentemente online attività come operazioni bancarie, prenotazioni per le prestazioni sanitarie e quelle della pubblica amministrazione, e ovviamente acquisti sulle piattaforme di e-commerce. Ma mentre l'intelligenza artificiale accelera la crescita del digitale, aumenta di pari passo anche la paura delle frodi informatiche. I numeri emersi recentemente dal rapporto annuale dell'Internet Crime Complaint Center (IC3) dell'FBI e dal nuovo Y-Report 2026 di Yarix fotografano infatti un contesto sempre più complesso. Negli USA le segnalazioni di crimini informatici sono aumentate del 26%, mentre gli attacchi ransomware a livello globale sono raddoppiati (+51%). Dietro questi dati, non c'è però soltanto un problema tecnologico, ma soprattutto una crisi di fiducia, causata sia dal cybercrime che dalla scarsa trasparenza delle stesse aziende, a cui spetta il compito di tutelare i dati dei propri clienti. A evidenziarlo sono rapporti autorevoli come il "Digital Trust Index 2026" di Thales, da cui è emerso che solo il 23% dei consumatori si fida delle aziende che utilizzano l'IA per gestire i propri dati, e solo il 16% afferma di comprendere chiaramente come le aziende raccolgono e utilizzano le loro informazioni personali, ricordando che per tali preoccupazioni l'82% degli utenti intervistati aveva già dichiarato di aver abbandonato almeno un brand nell'ultimo anno. Il vero rischio è la sfiducia digitale – Ogni attacco ransomware, ogni data breach, ogni truffa online non colpisce quindi soltanto aziende e infrastrutture, ma condiziona direttamente la percezione di sicurezza degli utenti. Questo significa meno propensione a utilizzare servizi online, minore disponibilità a condividere informazioni personali, e anche maggiore diffidenza verso applicazioni e strumenti basati sull'intelligenza artificiale. Pertanto, nelle aziende digitali la cybersecurity non è più soltanto una questione tecnica riservata agli specialisti IT, ma è diventata un fattore fondamentale che incide sulla fiducia dei clienti e sullo stesso business, motivo per cui dovrebbe interessare il management da vicino. Cybercrime industrializzato e utenti sempre più vulnerabili – Secondo il report dell'FBI, l'intelligenza artificiale sta inoltre abbassando drasticamente la soglia delle competenze tecniche necessaria per creare campagne fraudolente credibili: email di phishing scritte in modo impeccabile, deepfake con impersonificazioni realistiche, e truffe automatizzate sono ormai a portata di mano anche di hacker poco più che principianti. Questo cambia radicalmente il paradigma della sicurezza digitale a cui eravamo abituati negli ultimi anni. Limitarsi oggi a raccomandare di "fare attenzione" ai messaggi sospetti sarebbe come consigliare di non prendere caramelle dagli sconosciuti. Gli attacchi stanno diventando sempre più convincenti, personalizzati e difficili da riconoscere anche per utenti esperti. In parallelo, cresce anche la percezione di vulnerabilità. Compromissioni di account, furti di identità, truffe online sono ormai all'ordine del giorno, e vacillano anche sistemi che fino a poco tempo fa erano reputati sicuri, come l'autenticazione con dati biometrici dell'utente o quella a due fattori. In questo scenario in cui non ci sono più certezze di sicurezza assoluta, diventa sempre più difficile guadagnare la fiducia senza dimostrare un impegno concreto per tutelare gli utenti e offrire garanzie concrete sulle tecnologie messe a loro disposizione. La fiducia si costruisce con trasparenza e responsabilità – La percezione di sicurezza e fiducia non dipendono soltanto dall'utilizzo delle tecnologie di sicurezza più avanzate, ma soprattutto dal comportamento proattivo delle organizzazioni. Come denotano le statistiche, gli utenti oggi vogliono sapere come vengono trattati i loro dati, quali misure di sicurezza vengono adottate, come verranno gestiti eventuali data breach, e soprattutto desiderano comprendere se esiste un reale impegno nella protezione delle informazioni personali da parte delle aziende a cui si affidano, oppure se il rispetto della privacy viene solo sbandierato sotto forma di slogan per cercare di ingraziarsi i clienti. Oggi la vera sfida non è soltanto fermare i cybercriminali, o rincorrere il progresso tecnologico per rimanere competitivi, ma anche evitare che gli utenti perdano definitivamente la fiducia nel digitale, perché senza di essa nessuna innovazione può davvero funzionare in modo sostenibile.

Nicola Bernardi | Presidente di Federprivacy | @Nicola_Bernardi

PRIVACY News

EDITORE
Associazione Federprivacy

CODICE FISCALE
94156260484

PARTITA IVA
IT06413480481

REDAZIONE
Via Brunetto Degli Innocenti n. 2
50063 Figline Valdarno (FI) - Italy

INDIRIZZI
Via Brunetto Degli Innocenti n. 2
50063 Figline Valdarno (FI) - Italy
Numero Verde: 800 910 424
Email: urp@federprivacy.org
Web: www.federprivacy.org

DIRETTORE RESPONSABILE
Nicola Bernardi
presidenza@federprivacy.org

SEGRETARIO GENERALE
Davide Sottili
davide.sottili@federprivacy.org

SEGRETERIA DI REDAZIONE
Magda Todor
magda.todor@federprivacy.org

COMITATO REDAZIONALE
Nicola Bernardi, Marco Soffientini, Michele Iaselli, Michele Giannone, Vittorio Lombardi, Luisa Leone, Davide Sottili

STAMPATO DA
AGF S.r.l.
Via del Tecchione, 36 - Sesto Ulteriano
S. Giuliano Milanese (MI)

Testata registrata presso il Tribunale di Firenze Reg. N.5871 del 08.05.2012

Questa copia di Privacy News non è in vendita, ma è distribuita in Italia in direct mailing e spedita gratuitamente in esclusiva agli associati Federprivacy, nonché pubblicata online in versione sfogliabile sul sito www.federprivacy.org. Per scoprire come poterla ricevere e beneficiare di tutti gli altri vantaggi riservati ai soci Federprivacy visita il sito www.federprivacy.org, oppure scansionare il codice QR in questo riquadro:

FOCUS

PRIVACY E IA

PRIVACY E SOCIETÀ

PRIVACY IN AZIENDA

APPUNTAMENTI

Aumenta il **RISCHIO** globale sulla **CYBERSECURITY**: lo scorso anno **+26%** segnalazioni e **+51% RANSOMWARE**

> Secondo i dati raccolti dal **Security Operations Center**, nel 2025 sono stati monitorati oltre **522 mila eventi di sicurezza**, dei quali più di **158 mila** si sono **trasformati in incidenti** veri e propri

LEGGI ON-LINE

Il 2025 ha segnato un ulteriore aggravamento della minaccia cyber globale. I dati emersi dal rapporto annuale dell'Internet Crime Complaint Center (IC3) dell'FBI e dal nuovo Y-Report 2026 di Yarix restituiscono un quadro sempre più complesso: da un lato aumentano gli attacchi ransomware e le campagne di phishing sofisticate, dall'altro l'intelligenza artificiale e le criptovalute stanno diventando strumenti centrali nelle frodi online. I dati USA - Negli Stati Uniti, secondo il "2025 Internet Crime Report" dell'FBI, le perdite economiche legate ai crimini informatici hanno raggiunto quasi 21 miliardi di dollari, con oltre un milione di segnalazioni ricevute dall'IC3. Si tratta di un incremento di circa il 26% rispetto all'anno precedente. Le truffe legate alle criptovalute si confermano la categoria più dannosa. Le perdite attribuite a frodi crypto hanno superato gli 11 miliardi di dollari, trainate soprattutto da falsi investimenti, piattaforme inesistenti e schemi di social engineering sempre più convincenti. A rendere ancora più efficace il cybercrime è l'uso dell'intelligenza artificiale. Il rapporto FBI evidenzia come gli strumenti di IA generativa abbiano abbassato la soglia tecnica necessaria per costruire campagne fraudolente credibili. Nel solo 2025, le segnalazioni collegate a truffe che utilizzano l'intelligenza artificiale hanno superato le 22 mila unità, causando perdite per quasi 900 milioni di dollari. Tra le minacce più diffuse restano il phishing, le estorsioni digitali e le compromissioni di account. Il rapporto di Yarix - Parallelamente, il fenomeno ransomware continua a crescere su scala globale. Ed è proprio su questo punto che il rapporto Yarix offre una prospettiva particolarmente significativa per comprendere il contesto europeo e italiano. Secondo i dati raccolti dal Security Operations Center di Yarix, nel 2025 sono stati monitorati oltre 522 mila eventi di sicurezza, dei quali più di 158 mila si sono trasformati in incidenti veri e propri.

L'aumento medio mensile rispetto al 2024 è stato dell'8%, mentre gli eventi classificati come più gravi sono cresciuti del 62% su base annua. Il ransomware rappresenta la minaccia più critica.

La situazione in Italia - Il panorama italiano riflette molte delle dinamiche osservate negli Stati Uniti, ma con alcune peculiarità.

Secondo Yarix e i dati richiamati dall'Agenzia per la Cybersicurezza Nazionale, gli attacchi DDoS restano tra le tecniche più diffuse nel nostro Paese, seguiti da malware e attacchi ibridi. Nei primi sei mesi del 2025 sarebbero stati rilevati oltre 1.500 eventi cyber, con un incremento superiore al 50% rispetto all'anno precedente. Emergono inoltre con sempre maggiore evidenza le connessioni tra cybersicurezza e contesto geopolitico. Yarix evidenzia come hacktivismo, tensioni internazionali e conflitti digitali stiano contribuendo ad amplificare il livello di esposizione delle organizzazioni europee.

La minaccia non riguarda più soltanto il profitto economico, ma sempre più spesso obiettivi di destabilizzazione, propaganda o pressione politica. Sia il report FBI sia quello Yarix convergono su un punto fondamentale: il cybercrime sta diventando sempre più industrializzato.

Gli attacchi sono più automatizzati, più scalabili e più accessibili grazie all'utilizzo di strumenti di IA e piattaforme criminali "as a service". Questo consente anche a soggetti con competenze limitate di lanciare campagne sofisticate, aumentando il volume complessivo delle minacce. Il 2025 appare quindi come un anno spartiacque per la cybersecurity globale.

La combinazione tra ransomware, intelligenza artificiale e criptovalute sta ridefinendo il panorama del rischio digitale, mentre aziende e istituzioni si trovano a dover affrontare minacce sempre più trasversali, rapide e difficili da contenere. In questo scenario, la cybersicurezza non rappresenta più soltanto una questione tecnica, ma una componente strutturale della resilienza economica e istituzionale.

Fonte: Federprivacy

Con **INFORMATIVE** sulla **PRIVACY** **NON TRASPARENTI** si **PERDE** la **FIDUCIA** degli **UTENTI** e si **RISCHIANO** **SANZIONI** per violazioni del **GDPR**

Dopo decenni di privacy burocratica fatta di documenti da firmare senza neanche comprendere come fossero realmente utilizzati i loro dati personali, nel 2018 gli utenti avevano avuto la speranza di vedere finalmente un cambiamento con l'introduzione del GDPR, che nasceva con l'obiettivo dichiarato di restituire agli interessati il controllo sulle loro informazioni attraverso regole fondate su trasparenza, chiarezza e responsabilizzazione dei titolari del trattamento. Non è un caso che l'art. 12 del Regolamento UE 2016/679 imponga che le informazioni debbano essere fornite in forma "concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro". Eppure, a distanza di ben 8 anni dalla sua entrata in vigore, la realtà racconta purtroppo una storia ben diversa, e oggi sembra proprio di essere tornati al punto di partenza.

La trasparenza delle informative privacy tradita nella pratica - Nella maggioranza dei casi, le informative sulla privacy che attualmente popolano siti web, app, piattaforme di e-commerce e servizi di home banking sono infatti documenti lunghissimi, complessi e scritti in un gergo giuridico difficilmente comprensibile anche per utenti mediamente istruiti. E sarebbe riduttivo concludere che questa prassi diffusa rappresenti giusto un peccato veniale comunicativo delle aziende, perché in realtà costituisce una vera e propria violazione dello spirito – e spesso anche della sostanza – del GDPR. Uno studio di NordVPN ha evidenziato come una privacy policy sfiori mediamente le 7.000 parole, richiedendo circa 29 minuti per leggere un documento che in pratica è lungo circa 15/20 pagine di un testo che richiederebbe pure l'aiuto di un professionista per essere compreso bene. Considerando il numero medio di siti visitati ogni mese, un utente dovrebbe pertanto dedicare oltre 46 ore – più di una settimana lavorativa – per leggere tutte le informative. Non sorprende, quindi, che un italiano su tre scelga di non leggerle affatto.

> ***Uno studio di NordVPN ha evidenziato come una privacy policy sfiori mediamente le 7.000 parole, richiedendo circa 29 minuti per leggere e l'aiuto di un professionista per essere compreso bene***

I numeri della sfiducia digitale - Neanche si può pretendere di scaricare sbrigativamente tutte le responsabilità sulla pigrizia degli utenti, o su un loro generalizzato disinteresse per le tutele in materia di privacy, perché una recente indagine di NielsenIQ ha evidenziato che per il 69% dei consumatori la percezione di un corretto trattamento dei dati personali è un fattore determinante per affidarsi a un'azienda, e 7 italiani su 10 dichiarano di aver evitato almeno una volta l'accesso a un sito o a una app per non condividere le proprie informazioni. In realtà, la complessità della maggioranza delle policy supera ogni ragionevole aspettativa che rende materialmente impossibile una lettura consapevole delle politiche dei trattamenti di dati personali attuate da molte aziende. Anche se gli utenti sono rassegnati a subire tali dinamiche, ciò non significa che se trovassero un'alternativa non potrebbero decidere di rivolgersi a un altro fornitore di servizi di cui si fidano maggiormente. La trasparenza delle informative privacy come requisito giuridico - Sotto il profilo giuridico, la contraddizione è evidente: il GDPR impone trasparenza, ma la prassi operativa produce spesso opacità. E qui emerge un punto cruciale per i manager d'impresa: un'informativa lunga e incomprensibile non tutela l'azienda, ma la espone a rischi di vario genere, compresi quelli delle sanzioni che paradossalmente dovrebbe servire a evitare la pubblicazione di una privacy policy, ma anche quelli reputazionali del brand e della fiducia che l'utente dovrebbe avere per poter fare serenamente acquisti e fornire i propri dati personali ad una

piattaforma online. Gli articoli 13 e 14 del GDPR stabiliscono in modo dettagliato quali informazioni devono essere fornite agli interessati: finalità del trattamento, basi giuridiche, destinatari dei dati, tempi di conservazione, diritti esercitabili. Tuttavia, il legislatore europeo non ha mai richiesto che tali informazioni siano presentate in modo prolisso o tecnicamente oscuro. Al contrario, ha esplicitamente incoraggiato soluzioni innovative di semplificazione che sembrano essere state riposte in soffitta senza essere mai state neanche attuate. Le soluzioni dimenticate per informative più accessibili - Tra queste, il considerando 60 e lo stesso articolo 12 del Regolamento fanno riferimento all'utilizzo di icone standardizzate per rendere immediatamente comprensibili i contenuti essenziali. In questa direzione, anche il Garante per la protezione dei dati personali aveva promosso un contest per sviluppare simboli e soluzioni grafiche capaci di rendere le informative più accessibili. Un'iniziativa che, seppure lungimirante e fatta di buoni propositi, ha però visto la sostanziale indifferenza del mercato, e forse anche dagli stessi addetti ai lavori, che dopo l'assegnazione del premio ai vincitori è finita ben presto nel dimenticatoio. Perché la trasparenza delle informative privacy conviene alle aziende - Perché le aziende continuano allora a preferire informative complesse? La risposta è spesso legata a un gap culturale che non è mai stato colmato: avvocati e consulenti ritengono ancora che un linguaggio giuridico articolato e una maggiore lunghezza possano offrire maggiore protezione legale. In realtà accade l'opposto. Un'informativa che non è comprensibile viola il principio di trasparenza e può essere considerata non conforme al GDPR, con il rischio di sanzioni e contenziosi. Ma non è solo una questione normativa. È anche – e soprattutto – una questione di fiducia. In un contesto digitale sempre più competitivo, la fiducia degli utenti rappresenta un asset strategico. Informative lunghe, oscure e piene di tecnicismi generano diffidenza. Al contrario, comunicazioni chiare e trasparenti rafforzano la relazione tra azienda e cliente. Questo è particolarmente rilevante in settori come il web banking, l'e-commerce e i servizi digitali avanzati, dove la condivisione dei dati è inevitabile e la fiducia diventa un fattore competitivo decisivo.

Come invertire questa tendenza?

Come rendere reale la trasparenza delle informative privacy - La prima leva è culturale: occorre abbandonare una visione burocratica della compliance e adottare un approccio orientato all'utente. L'informativa non deve essere un documento difensivo, ma uno strumento di comunicazione più simile a una "carta dei servizi" che l'azienda dovrebbe sfoggiare con orgoglio per rendere noto il suo impegno nel rispettare la privacy dei propri clienti. In questa prospettiva, l'elaborazione di una privacy policy ben fatta deve essere affidata a un giurista che, oltre ad essere ferrato nella normativa, abbia anche spiccate capacità comunicative e lessicali. Buone pratiche operative per informative più chiare - Dal punto di vista operativo, alcune buone pratiche possono fare la differenza sono le seguenti: 1. Sintesi e struttura: utilizzare livelli informativi, con una prima sintesi chiara e approfondimenti accessibili tramite link. 2. Linguaggio semplice: evitare il legalese e privilegiare frasi brevi, esempi concreti e terminologia comprensibile. 3. Visualizzazione: integrare icone, infografiche e schemi per facilitare la lettura. 4. Trasparenza reale: evidenziare in modo chiaro gli aspetti più rilevanti per l'utente, come la condivisione con terze parti o finalità di marketing. 5. User experience: progettare l'informativa come parte integrante dell'esperienza utente, non come un ostacolo da superare. 6. Non ricorrere a sotterfugi per il solo scopo di persuadere l'interessato a dare un consenso in realtà non consapevole. Test di comprensione e rischi reputazionali - Per fugare ogni dubbio, la riprova empirica per essere certi che un'informativa rispecchi realmente i requisiti del GDPR è quella di sottoporla a un campione di diretti interessati a cui deve essere rivolto il testo, chiedendo loro se lo comprendono bene, oppure se necessitano di alcuni chiarimenti. Inoltre, è fondamentale contrastare pratiche scorrette come i cosiddetti "dark pattern", e la "privacy fatigue", utilizzate da molte piattaforme che mirano solo a estorcere consensi agli utenti e indurli ad accettare passivamente policy che celano cavilli legali studiati ad arte per legittimare il massimo sfruttamento dei dati personali, ignorando però che tale approccio comporta in realtà un clamoroso effetto boomerang che mina la fiducia degli stessi utenti ed espone alle sanzioni delle autorità. Infatti, queste pratiche sono sempre più nel mirino delle autorità di controllo e rischiano di compromettere seriamente la reputazione aziendale. La trasparenza delle informative privacy misura la vera compliance - Per molti anni è stato affermato che il GDPR non è solo un insieme di obblighi da rispettare, ma rappresenta piuttosto un'opportunità, ma sono ancora pochissime le aziende che hanno saputo coglierla, trasformando la protezione dei dati da costo a leva strategica. Occorre quindi tenere presente che la vera compliance non si misura sulla lunghezza delle informative, ma sulla loro capacità di essere comprese. E senza chiarezza e trasparenza non può esserci né compliance né fiducia, fattori indispensabili per rimanere competitivi nel mercato digitale.

Agenda Digitale
Articolo di Nicola Bernardi, Presidente di Federprivacy

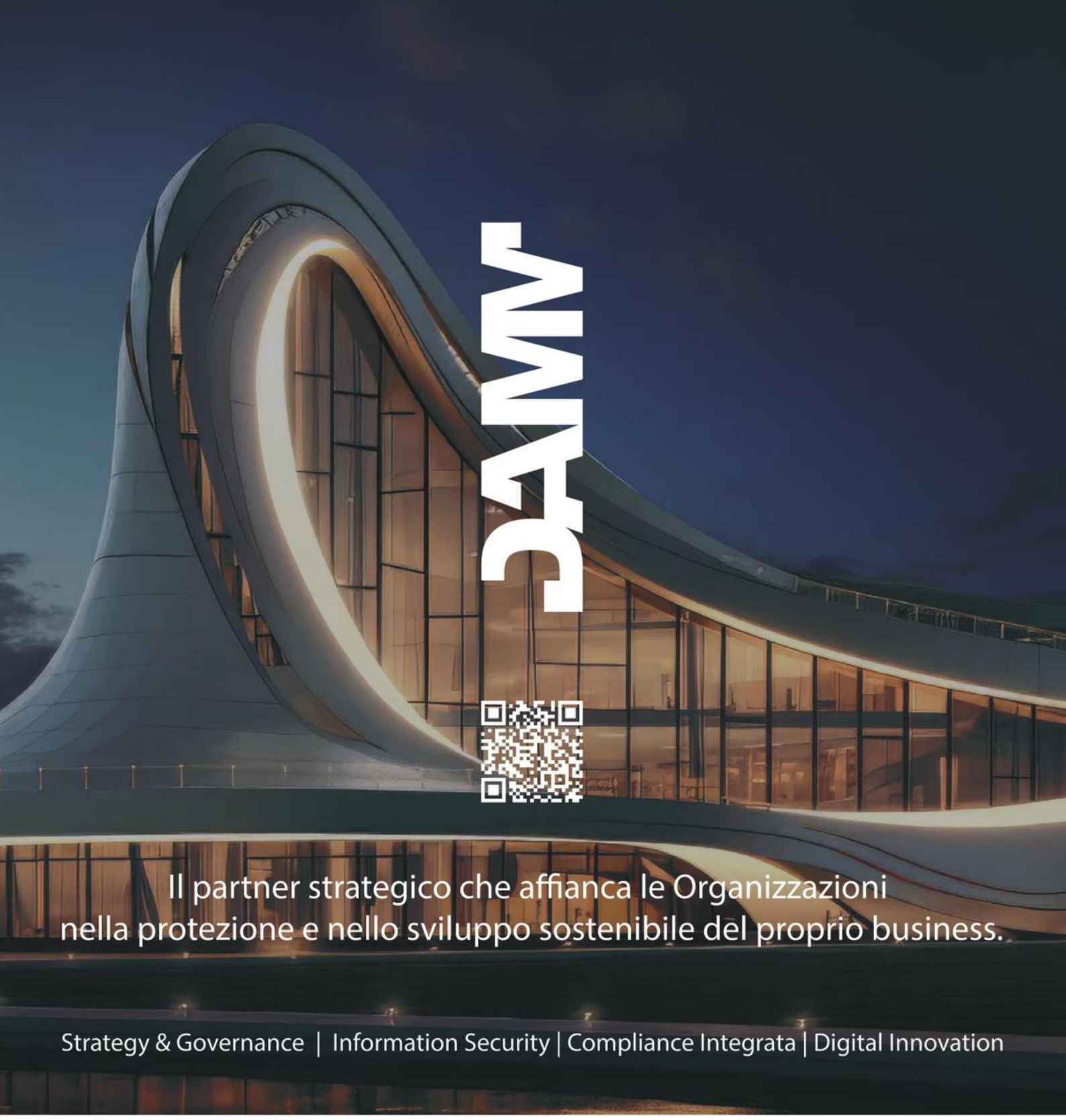
MERCATI DIGITALI, PRIVACY e **DATI PERSONALI** entrano nel perimetro dell'intervento **ANTITRUST**

> La **protezione dei dati personali** non è più solo una questione di diritti fondamentali, ma **entra** a pieno titolo **negli strumenti di regolazione del mercato**

Da anni sentiamo dire che "se un prodotto è gratis, allora il prodotto sei tu", a rimarcare che sempre più spesso nel mercato digitale il prezzo è rappresentato dai nostri dati personali.
È su questo terreno che la data economy sta intrecciando sempre di più i ruoli delle varie autorità di vigilanza, ridefinendo anche quello dell'Autorità Garante della Concorrenza e del Mercato (AGCM), oggi chiamata a intervenire in ambiti che fino a pochi anni fa sembravano riservati al Garante per la protezione dei dati personali. Se nel capitalismo delle piattaforme il valore non si misura soltanto in euro, ma anche nella capacità di raccogliere, analizzare e sfruttare le informazioni degli utenti, nell'era digitale l'Antitrust non si limita più a vigilare sui prezzi, ma "invade" il perimetro della privacy.
Ad evidenziarlo, è l'ultima relazione annuale di AGCM presentata alla Camera dei Deputati lo scorso 14 aprile. Tra le varie decisioni assunte dall'Antitrust nei confronti dei colossi tecnologici, emblematica è la sanzione da oltre 100 milioni di euro inflitta a Google per abuso di posizione dominante nel caso Google Shopping, dove l'Autorità ha contestato l'esclusione di un'app concorrente nel mercato dei servizi per la ricarica dei veicoli elettrici. Un intervento che, pur formalmente antitrust, ruota attorno al controllo dei dati e degli ecosistemi digitali.
Non meno significativo è il procedimento dello scorso dicembre in cui AGCM ha imposto una sanzione di circa 100 milioni di euro ad Apple per aver ostacolato l'acquisizione del consenso necessario alla profilazione degli utenti da parte degli sviluppatori di app, mediante l'imposizione di condizioni non oggettive, non trasparenti e non proporzionate all'esigenza di garantire il rispetto della normativa in materia di privacy. Ma è soprattutto sul fronte della tutela del consumatore che l'AGCM ha iniziato a presidiare in modo più diretto l'uso dei dati personali, come nel caso della sanzione da 7 milioni di euro inflitta a Meta, in cui l'Autorità ha contestato pratiche ingannevoli legate alla presentazione dei servizi come "gratuiti", senza adeguata informazione sul valore economico dei dati ceduti dagli utenti, assumendo una posizione che segna un passaggio culturale importante, perché riconosce esplicitamente il dato personale come controprestazione alla stregua del denaro. Il Garante per la protezione dei dati personali cede quindi il passo all'Antitrust quando l'asimmetria informativa sul trattamento dei dati altera la libertà di scelta del consumatore, o quando il controllo dei dati rafforza posizioni dominanti difficilmente contendibili. In questo scenario, il confine tra competenze dell'AGCM e quelle del Garante per la privacy diventa però sempre più sottile. Se quest'ultimo continua a presidiare la liceità del trattamento dei dati, l'Autorità antitrust si concentra sugli effetti economici e competitivi del loro utilizzo, dando vita a una forma di convergenza regolatoria che appare destinata a rafforzarsi.
Il punto di svolta è ormai evidente: nei mercati digitali non si può più mirare soltanto e tutelare la riservatezza dell'individuo, ma occorre anche garantire che l'uso dei dati non alteri il funzionamento del mercato.
Questo cambio di paradigma che caratterizza il digitale apre sicuramente nuove opportunità di tutela, ma anche interrogativi sul coordinamento tra autorità e sulla necessità di evitare sovrapposizioni, e per questo lo scorso anno AGCM e Garante Privacy hanno firmato un protocollo di collaborazione reciproca. E l'evoluzione non è solo italiana. Il quadro europeo, con il Digital Markets Act e il Digital Services Act, va nella stessa direzione: limitare il potere delle grandi piattaforme intervenendo anche sui meccanismi di raccolta e utilizzo dei dati. Tuttavia, l'esperienza dell'AGCM mostra come già oggi, anche in assenza di strumenti settoriali pienamente operativi, sia possibile utilizzare il diritto della concorrenza e la tutela del consumatore per incidere su questi fenomeni.

LEGGI ON-LINE

Fonte: Economy – Articolo di Nicola Bernardi, Presidente di Federprivacy



DAMM è la società di consulenza direzionale che nasce nel 2019 dall'esperienza consolidata del proprio management maturata all'interno di multinazionali leader globali nella **consulenza strategica e tecnologica.**

DAMM

DAMM srl
Via S'Arrulloni n.10, 09126 Cagliari,
P.IVA: 03860880925

https://dammsec.com

Build to Lead

EvoPrivacy
by Evolutivo.io

Evolutivo SRL | Italy Spain Albania Tanzania

L'Abilitatore che amplifica la tua consulenza

L'Ufficio Privacy Esterno a Tua Disposizione

Compliance

Compliance Platform

Business Continuity

Cybersecurity

Audit e Monitoraggio

Training

Governance

Sei un DPO o un Consulente Privacy
Scopri il nostro Partner Program

EvoPrivacy è il braccio operativo specializzato nell'esecuzione di tutti i processi di conformità GDPR, NIS2 e cybersecurity: lavora su indicazione del DPO o del Consulente Privacy, garantendo che ogni direttiva venga concretamente attuata al posto del cliente, con precisione e continuità. Le aziende che non dispongono ancora di uno specialista privacy trovano in EvoPrivacy anche il punto di accesso per strutturare il percorso corretto. Un solo interlocutore operativo, per tenere tutto sotto controllo.

Test Gratuito
Valutazione preliminare di adeguatezza

evoprivacy@evolutivo.io
www.evoprivacy.it | www.evolutivo.io

Gli **ALGORITMI** stanno **RUBANDO** i vostri **DATI BANCARI**, ma non come pensate

> Non si tratta di un caso italiano: in Europa **i colossi bancari usano l'AI per ottimizzare le proprie campagne di marketing predittivo**, analizzando i dati in tempo reale per anticipare i bisogni dei clienti e prevederne i comportamenti di spesa

Di recente, la scure del Garante della privacy si è abbattuta su Intesa Sanpaolo con una multa da 17,6 milioni di euro, fino a quel giorno la più pesante mai inflitta in Italia per violazioni della privacy nel settore bancario, alla quale poco dopo ne ha fatto seguito un'altra di addirittura 31,8 milioni di euro, per un totale di quasi 50 milioni di euro di sanzioni inflitte al noto istituto bancario italiano nel giro di pochi giorni. Se nel secondo caso il provvedimento riguardava gravi carenze nella sicurezza dei dati personali dovute all'inadeguatezza delle misure tecniche e organizzative adottate, invece relativamente alla prima multa le cause non erano riconducibili ad hacker o furti notturni, ma ad un'operazione interna effettuata dallo stesso gruppo bancario, che ha spostato arbitrariamente 2,4 milioni di clienti verso la propria banca digitale "Isybank".

Come è potuto accadere? attraverso l'uso di algoritmi che hanno scandagliato dati personali – età, abitudini online, portafoglio investimenti – per decidere chi doveva essere migrato alla banca digitale e chi no. Non sulla base di un vero consenso dato dal cliente, bensì con un silenzio-assenso camuffato da comunicazioni vaghe, inviate tramite app durante l'estate, quando notoriamente si è meno attenti. Per questo, il Garante ha parlato di "profilazione illecita", ovvero trattamenti di dati automatizzati che valutano aspetti personali con effetti concreti, come il cambio dell'iban o la perdita all'accesso alle filiali fisiche. Anche se la banca aveva sostenuto di essersi basata su criteri definiti da esseri umani, negando di aver agito sulla base di decisioni puramente automatiche, pare però chiaro che a fare il grosso di un lavoro su così vasta scala siano stati proprio gli algoritmi. E non è un caso isolato nel mondo bancario italiano, dove questi sistemi, spesso potenziati dall'AI, non rubano soldi dal vostro conto, ma interagiscono sul loro controllo. Immaginate di entrare in un'applicazione bancaria e vi viene proposto un mutuo prima ancora di chiederlo.

Non è telepatia: è machine learning che fruga tra estratti conto, pattern di spesa, e persino acquisti che indicano cambiamenti del vostro tenore di vita. Il punto è che non avete firmato nulla di nuovo.

Il consenso è sepolto in contratti vecchi di anni, una check-box che avete spuntato distrattamente anni addietro, quando invece il GDPR dovrebbe tutelarvi e assicurarvi che i vostri dati vengano trattati in modo lecito e trasparente.

Nel caso Intesa, il Garante ha respinto l'interesse legittimo invocato dalla banca, reputandolo una valutazione superficiale che non bilanciava realmente i diritti dei clienti. Mancavano informative chiare.

E la profilazione? qualificata come automatizzata, anche se non da AI avanzata, perché estrapola e classifica dati su larga scala, con impatti reali. Se dite no, rischiate di essere penalizzati con limiti ridotti o offerte peggiori. È "personalizzazione", dicono. È sorveglianza, pensano in molti.

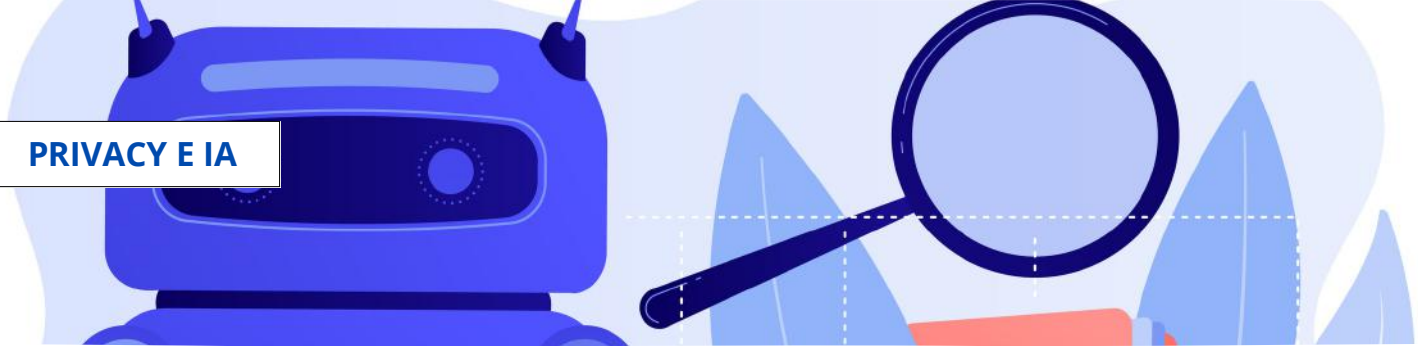
Nel 2025, Intesa ha chiuso con un utile netto di 9,3 miliardi di euro, in crescita del 7,6%. Quindi una multa da 17,6 milioni è un graffio, e non una ferita. Ma il danno vero è sulla fiducia. Se a vostra insaputa un algoritmo vi classifica ad "alto rischio" – magari per pattern invisibili come acquisti online notturni – e vi alza il tasso, non potrete contestarlo. Questi modelli sono black box opache, protette come segreti industriali. Il cliente ignora quale sia la logica adottata e come vengano veramente usati i suoi dati.

E in caso di errore? nella vicenda di Isybank ci sono stati migliaia di reclami di clienti over 65 spostati per sbaglio, e famiglie che hanno perso servizi per loro essenziali.

Ora però anche il Garante italiano ha alzato l'asticella, e i CEO bancari sono a un bivio: continuare senza farsi troppi scrupoli a spingere una tecnologia che anticipa il cliente oppure investire in compliance vera, con la messa disposizione di dashboard dove il cliente vede cosa la banca sa di lui, nonché opt-out facili e algoritmi verificabili.

LEGGI ON-LINE

Fonte: Economy - Articolo di Mario Mosca, Coordinatore Gruppo di Lavoro Federprivacy per la Privacy nel settore Bancario e Finanziario



L'**INTELLIGENZA ARTIFICIALE** non è una **QUESTIONE TECNOLOGICA**, ma di **GOVERNANCE**

> La **protezione dei dati entra nel cuore della governance dell'AI**. Non è più sufficiente verificare la base giuridica del trattamento ma **occorre presidiare l'intero ciclo di vita del dato**

L'intelligenza artificiale sta rapidamente penetrando nei processi aziendali, ma fermarsi alla dimensione tecnologica rischia di essere fuorviante.
A differenza di come si potrebbe pensare, il vero tema non è infatti tecnologico, ma organizzativo.
L'AI non può essere trattata come un progetto IT: è, a tutti gli effetti, un processo aziendale strutturato, che richiede responsabilità diffuse e un sistema di controllo che accompagni il suo intero ciclo di vita.
Il punto di partenza non è la tecnologia, ma il business. Ogni iniziativa nasce da un'esigenza concreta e da un responsabile preciso: il "business owner", a cui spetta individuare l'opportunità e ad assumerne la responsabilità, trasformando l'AI da semplice sperimentazione tecnica a leva industriale.
Intorno a questa figura si attiva poi una vera e propria architettura organizzativa: una funzione tecnica deputata allo sviluppo ("AI Factory") affiancata da strutture di governance che presidiano regole e rischi, oltre a un sistema di comitati chiamati ad approvare e monitorare le iniziative.
Non si tratta, dunque, di innovazione "libera", ma di innovazione governata. Ed è proprio qui che si coglie uno dei principali cambi di paradigma. Prima ancora di sviluppare o adottare un algoritmo, l'azienda è chiamata a interrogarsi sul rischio.
Non è un passaggio formale, ma sostanziale: si tratta di valutare in anticipo se e in che misura un sistema possa generare impatti rilevanti, considerando cosa fa, come opera, su chi incide e con quale livello di criticità.
Questo approccio anticipatorio è sempre più centrale anche alla luce del quadro normativo europeo.
Con l'entrata in vigore dell'Artificial Intelligence Act, le imprese sono infatti chiamate a classificare i sistemi in base al rischio e a rispettare obblighi proporzionati. Ma è soprattutto il coordinamento con il Regolamento generale sulla protezione dei dati (GDPR) a rappresentare il vero banco di prova operativo.
L'intelligenza artificiale, infatti, è quasi sempre data-driven: funziona tanto meglio quanto più i dati sono ampi, accurati e aggiornati. Ed è proprio qui che si annidano alcuni dei rischi più rilevanti. Basti pensare che, secondo uno studio condotto dal USC Information Sciences Institute, circa il 40% dei dataset utilizzati nei modelli di AI presenta problemi di qualità, bias o incompletezza, con effetti diretti sull'affidabilità delle decisioni automatizzate. La protezione dei dati entra quindi nel cuore della governance dell'AI. Non è più sufficiente verificare la base giuridica del trattamento o adempiere agli obblighi informativi, ma occorre presidiare l'intero ciclo di vita del dato. Questo significa, ad esempio, interrogarsi sulla provenienza dei dati utilizzati per addestrare i modelli, sulla loro rappresentatività, sulla presenza di eventuali distorsioni e sulla compatibilità degli utilizzi con le finalità originarie.
Il principio che emerge è netto: se il rischio è troppo elevato o non adeguatamente gestibile, il progetto non deve partire. È un'inversione rispetto al passato, in cui il controllo interveniva spesso a valle. Oggi, invece, la decisione si deve prendere a monte.
Da qui deriva anche un'altra conseguenza: l'intelligenza artificiale non è un evento, ma un processo continuo. Il suo ciclo di vita attraversa diverse fasi – dalla valutazione iniziale allo sviluppo, fino alla messa in produzione e alla gestione operativa – ma ciò che conta è la continuità del presidio. Nessun algoritmo può essere semplicemente "rilasciato" e dimenticato. In questo contesto cambia profondamente anche il ruolo della compliance. Non è più una funzione chiamata a verificare ex post, ma un attore che entra nel processo decisionale, contribuisce alla valutazione del rischio, esprime pareri formali e, se necessario, può anche bloccare o condizionare un'iniziativa. E non opera in isolamento: il controllo diventa distribuito, coinvolgendo privacy, risk management, sicurezza informatica e altre funzioni chiave.
.... continua a leggere online

CONTINUA ON-LINE LA LETTURA

Fonte: Economy – Articolo di Davide Panella

FIDUCIA, EQUITÀ e TRASPARENZA: l'AI come nuovo PATTO tra BANCA e CLIENTE

> La figura del **DPO** e quella delle **funzioni di risk management** si stanno **trasformando: da ruoli tecnici** o normativi **a ruoli di governance etica**, capaci di interpretare rischi nuovi, promuovere cultura e guidare l'adozione responsabile dell'AI nel sistema bancario

CONTINUA ON-LINE LA LETTURA

Nel 2026 l'intelligenza artificiale è diventata infrastruttura critica del settore bancario. Dal credit scoring alla prevenzione delle frodi, fino ai processi HR, l'AI non è più un elemento sperimentale ma inizia ad essere parte integrante dei processi decisionali. Parallelamente, il quadro regolatorio europeo, AI Act in primis, spinge verso un modello di utilizzo dell'AI basato su responsabilità, trasparenza e tutela dei diritti fondamentali. In questo scenario, la sfida per il mondo bancario non è scegliere tra innovazione e compliance: è costruire un ecosistema in cui l'AI generi valore economico rafforzando la fiducia dei clienti e dei regolatori. La fiducia del cliente nell'AI: il nuovo capitale reputazionale delle banche - La trasformazione portata dall'intelligenza artificiale nel settore bancario non riguarda solo l'efficienza. Con l'AI Act, la relazione tra banca e cliente cambia in profondità: la fiducia diventa un vero asset competitivo. E qui non dobbiamo dimenticare un elemento fondante del settore finanziario: il valore fiduciario della relazione banca cliente. Una banca non offre solo servizi, ma prende decisioni che possono avere "effetti giuridici che riguardano la persona o incidere in modo analogo sulla sua vita", per richiamare la formulazione dell'art. 22 del GDPR sulle decisioni basate su trattamenti automatizzati. Questo principio, già presente nel GDPR, diventa ancora più centrale nell'era dell'AI: il cliente deve poter confidare che le decisioni che lo riguardano, che si tratti di credito, antifrode, onboarding, valutazioni interne o, ancora, sistemi conversazionali basati su AI siano comprensibili, controllabili e contestabili.

Il regolatore introduce obblighi di trasparenza, qualità dei dati, tracciabilità, verificabilità e supervisione umana, che non sono meri adempimenti tecnici, ma condizioni per garantire equità e responsabilità. Non basta più implementare modelli rapidi e performanti. Serve poter spiegare perché un sistema propone una decisione, mostrarne la correttezza, e assicurare che non produca effetti discriminatori.

La vera metrica competitiva non è più la velocità del modello, ma la credibilità del processo decisionale.
Tre elementi diventano cruciali:
- trasparenza percepita. Il cliente vuole capire come e perché viene presa una decisione che lo riguarda (es. merito creditizio). La trasparenza è anche comunicazione chiara;
- verificabilità. Modelli misurabili, auditabili e tracciabili: la banca deve poter dimostrare l'assenza di errori sistemici, distorsioni o bias. La fiducia nasce dalla capacità di "mostrare le prove";
- qualità dei dati e responsabilità del trattamento. Una banca che gestisce correttamente i dati, attraverso misure tra cui minimizzazione, finalità chiare e filiere controllate, trasmette valore e affidabilità.

L'AI come asset reputazionale - Un algoritmo opaco genera sospetto. Un algoritmo spiegabile, controllato e stabile genera fiducia. Nel banking, questa dinamica è amplificata: il cliente accetta decisioni da parte della propria banca solo se percepisce che:
- esiste una supervisione umana reale;
- la decisione è comprensibile e contestabile;
- il sistema è progettato per proteggere i suoi diritti.

L'AI diventa quindi un elemento di reputazione, come la sicurezza informatica, la privacy, o la solidità finanziaria. Le banche che sapranno usare l'AI con responsabilità, trasparenza e equità saranno più competitive nel lungo periodo. Explainability come diritto e vantaggio competitivo - L'AI Act richiede spiegazioni comprensibili per i sistemi high risk. Le banche devono introdurre standard interni di explainability, rendendo le decisioni leggibili anche ai non esperti. La trasparenza diventa parte dell'esperienza cliente. La supervisione umana deve essere effettiva, non simbolica, i clienti la richiedono già oggi. Risulta quindi necessario garantire capacità di intervento; competenze adeguate; responsabilità definite e monitoraggio continuo del comportamento dei modelli.

.... continua a leggere online

Fonte: Articolo di Daniela Donati, Data Governance & Protection Expert di ING Italia

PRIVACY SUPPORT CENTER

Interact with stakeholders, *easily*

Il **Privacy Support Center** è un **servizio** pensato per offrire alle **organizzazioni** un punto di riferimento **unico** e **centralizzato** in materia di **protezione dei dati personali** e **sicurezza delle informazioni**.

Attraverso un **portale web** dedicato o integrato direttamente al **sito istituzionale** del Cliente, consente di comunicare in modo **trasparente** con tutti gli **stakeholder** interessati, semplificando l'accesso alle **informazioni** e la gestione dei **diritti** sia in ambito **nazionale** che **internazionale**.

Grazie a un'interfaccia **chiara** e **personalizzabile**, gli utenti possono consultare le **policy aziendali** in materia di **privacy** e **cybersecurity**, **esercitare i propri diritti** tramite **moduli guidati**, **segnalare violazioni dei dati**, **contattare i referenti interni** (come il **DPO** o il **Rappresentante** nelle varie legislazioni UE, UK, CH, TR, EG, CN, TH), nonché visionare **certificazioni**, **attestazioni** e **contenuti informativi**.

PERCHÈ SCEGLIERE
il Privacy Support Center

- rafforza l'**accountability**
- consolida la **fiducia** degli interessati
- garantisce una **governance dei dati** più efficace, reattiva e accessibile.

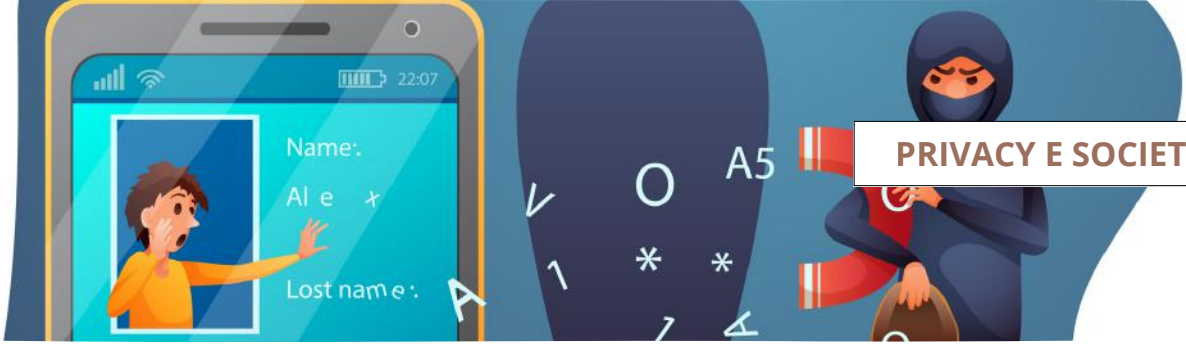
- Infrastruttura **cloud conforme al GDPR** (ISO 27001, ISO 27701, SOC 2 Type 2)
- Accessi con **autenticazione sicura** 2FA
- **Logging** delle attività e **tracciamento** delle **interazioni**

CARATTERISTICHE

- Portale Web dedicato o integrabile nel sito del Cliente
- Segnalazioni di Data Breach o Incidenti Informatici
- Area certificazioni, audit e policy
- Area Informative
- Contatti e funzioni di supporto (DPO, Rappresentante, ecc.)
- Portale multilingua
- Esercizio dei Diritti degli Interessati
- Knowledge Base personalizzabile
- Personalizzazioni e aggiornamenti

365 TRUST.me
business@365trust.me
800 172 542
privacysupport.center

SCOPRI DI PIÙ



Ecco quali sono le **20 APP PIÙ INTRUSIVE** per la **PRIVACY** degli **UTENTI**

> Alcune app raccolgono informazioni senza condividerle con terze parti, altre non tracciano affatto dati personali, ma **molte** altre **raccolgono dati personali e spiano gli utenti**

Nel dibattito sulla privacy digitale, l'intrusività delle app non è più limitata ai social network, ma riguarda l'intero ecosistema. Con 16 milioni di italiani che utilizzano almeno un'app (il 35% della popolazione), diventa sempre più importante conoscere cosa si sta condividendo. Sebbene molte applicazioni forniscano servizi utili, raccolgono anche quantità significative di dati personali: informazioni sugli acquisti, cronologia di navigazione e ricerca, dati personali, posizione Gps, contenuti creati dagli utenti, informazioni finanziarie, salute e fitness. Alcune app raccolgono queste informazioni senza condividerle, altre non tracciano affatto, ma molte altre raccolgono dati e spiano gli utenti, rendendo fondamentale sapere quanto si sta realmente condividendo prima di installarle. Una ricerca pubblicata da Truffa.net ha analizzato le informative sulla privacy delle app più popolari in Italia, mostrando come la raccolta dei dati sia diventata una componente strutturale delle piattaforme, indipendentemente dal settore. I dati evidenziano una doppia direttrice: da un lato l'utilizzo interno, che supera mediamente l'80% per miglioramento dei servizi e ottimizzazione degli algoritmi, e dall'altro la condivisione con terze parti, che oltrepassa il 60% per finalità pubblicitarie. È proprio questo equilibrio a definire il grado di intrusività delle diverse applicazioni. In cima alla classifica si collocano i social network, il cui modello economico si fonda sulla profilazione. Le piattaforme del gruppo Meta — Facebook, Messenger, Instagram e Threads — raggiungono livelli elevatissimi, fino al 68,6% dei dati condivisi con esterni e oltre l'85% utilizzato internamente, superando il 90% in alcune categorie per un sistema pervasivo basato su una raccolta continua. LinkedIn presenta invece una condivisione più contenuta, intorno al 37,1%, ma compensa con un utilizzo interno molto elevato che supera il 68%, manifestando la sua intrusività nell'elaborazione approfondita dei dati. Un profilo simile, ma più equilibrato, si osserva in Pinterest, dove il 42,9% dei dati viene condiviso e percentuali superiori al 70% emergono in alcune voci di utilizzo interno.

Passando ad altri settori, Amazon Shopping mostra una condivisione diretta più limitata, dal 5,7% al 25,7%, ma evidenzia un uso interno consistente e superiore al 54%, con picchi del 68,6% nella profilazione per anticipare i comportamenti d'acquisto. Nel campo dei contenuti digitali, YouTube presenta un modello intermedio, con circa un terzo dei dati condiviso e quasi la metà utilizzato per finalità interne. Tra i social fuori dal gruppo Meta, X mantiene livelli medi con il 28,6% di condivisione e valori complessivi tra il 37% e il 51%, mentre TikTok presenta una distribuzione disomogenea, dove alcune categorie scendono sotto il 20% e altre raggiungono il 62,9%, segnalando una raccolta selettiva ma incisiva. Le piattaforme di servizi quotidiani come Uber Eats, Uber e Deliveroo mostrano livelli di raccolta elevati fino al 60%, ma una condivisione talvolta nulla in alcune categorie, poiché il valore dei dati risiede nella capacità di descrivere abitudini e spostamenti internamente. Nel settore finanziario, PayPal evidenzia una dinamica peculiare con una raccolta iniziale contenuta ma un utilizzo dei dati che cresce fino al 65,7% in alcune categorie, mostrando cautela nella condivisione ma un uso intensivo per sicurezza e analisi. Le app di navigazione, come Waze e Google Maps, mostrano un'intrusività legata alla funzionalità, mantenendo la raccolta su livelli medi ma raggiungendo picchi elevati per i dati di geolocalizzazione e traffico. Infine, servizi come Spotify, Gmail, Bumble e Just Eat presentano percentuali superiori al 50% in specifiche aree, confermando che nessuna categoria è estranea alla logica della profilazione. Ciò che emerge complessivamente è che non esistono piattaforme neutrali, ma modelli differenti di sfruttamento dei dati attraverso l'estensione delle condivisioni o l'uso interno intensivo. Resta tuttavia aperta la questione della trasparenza richiesta dal GDPR poiché, nonostante la disponibilità delle informative, la comprensione reale dei meccanismi resta limitata, lasciando gli utenti in una posizione di controllo solo teorico e ridefinendo il tema centrale nella ricerca di un equilibrio sostenibile tra innovazione e tutela della privacy.

LEGGI ON-LINE

Fonte: Truffe.net

DPO SUITE

Lo strumento completo per la compliance su misura

DPOSuite è la piattaforma digitale che supporta organizzazioni pubbliche e private nella valutazione e gestione dei rischi legati ad IA e dati personali con elevata accuratezza.

Nel rispetto del Regolamento (UE) 2024/1689 (AI Act), del GDPR e delle Linee Guida AgID 2025.

- Conformità normativa: pieno allineamento ad AI Act, GDPR, Linee Guida AgID 2025 e WP248
- Percorsi guidati per semplificare i tuoi processi di valutazione
- Definizione e tracciabilità di ruoli e governance
- KPI e monitoraggio sempre a portata di mano
- Supporto alla compilazione anche per chi non ha formazione giuridica o tecnica

Richiedi una demo e approfitta della **Promo Early Access** riservata ai Soci Federprivacy e ai partecipanti del Privacy Day Forum!

Vai su www.dposuite.it o inquadra il QR Code

BYOD e **APP** di **MONITORAGGIO** in **AZIENDA**: rischi e misure organizzative

> Sul piano organizzativo, il principio di minimizzazione impone alle aziende di adottare un approccio di **Privacy by Design** e **Privacy by Default** nello sviluppo o nella selezione di qualsiasi applicazione o sistema di monitoraggio

L'Agenzia Spagnola per la Protezione dei Dati (AEPD) ha inflitto una sanzione di 200.000 euro alla società Ares Capital S.A., operante nel settore del trasporto privato con conducente, per aver obbligato i propri dipendenti-autisti a installare fino a quattro applicazioni di monitoraggio sui loro dispositivi mobili personali. Il procedimento sanzionatorio si era aperto a seguito della denuncia presentata il 23 luglio 2024 da un lavoratore della compagnia. Le applicazioni richieste dall'azienda consentivano la raccolta sistematica e continua di dati dei lavoratori ben oltre le esigenze operative: geolocalizzazione in tempo reale, messaggi e chiamate, fotografie, registrazioni audio e video, nonché dati relativi allo stato fisico e alla salute dei conducenti. Era inoltre vietato ai dipendenti di modificare qualsiasi impostazione o permesso delle applicazioni stesse. Il Garante spagnolo ha individuato e sanzionato tre distinte violazioni del GDPR:

- violazione del principio di minimizzazione
- mancanza di una base giuridica valida per il trattamento
- inadempimento dell'obbligo di informazione trasparente ai lavoratori

In questo articolo vogliamo illustrare alcune misure organizzative per prevenire un evento come quello descritto.

Politiche BYOD (Bring Your Own Device) e MDM - L'utilizzo di dispositivi personali del lavoratore per scopi professionali — prassi sempre più diffusa — richiede la predisposizione di una specifica politica aziendale (Policy BYOD) che deve prevedere:

- delimitare con precisione i dati di origine aziendale che possono essere trattati sul dispositivo personale e per quali finalità;
- garantire la separazione logica (containerizzazione) tra l'ambiente aziendale e quello privato del dispositivo;
- adottare soluzioni di Mobile Device Management (MDM) proporzionate e trasparenti, con la certezza che i software di gestione agiscano esclusivamente sull'area aziendale del dispositivo;
- garantire il diritto alla disconnessione digitale al termine dell'orario di lavoro, come richiesto esplicitamente dalla stessa AEPD nel provvedimento in esame.

Il principio di minimizzazione come vincolo di progettazione - L'infrazione più gravemente sanzionata nel caso Ares Capital riguarda la raccolta eccessiva di dati.

Le applicazioni aziendali richiedevano l'accesso a microfono, fotocamera, archivio fotografico, stato fisico e geolocalizzazione continua, laddove la prestazione del servizio di trasporto avrebbe richiesto al più la geolocalizzazione durante la corsa e alcune funzionalità di comunicazione. Sul piano organizzativo, il principio di minimizzazione impone alle aziende di adottare un approccio di Privacy by Design e Privacy by Default nello sviluppo o nella selezione di qualsiasi applicazione o sistema di monitoraggio.

Le configurazioni predefinite devono garantire il trattamento del minor numero di dati possibile, e ogni permesso aggiuntivo deve essere giustificato da una specifica necessità operativa documentata.

Prima di adottare qualsiasi soluzione tecnologica di monitoraggio, è indispensabile effettuare una mappatura dei flussi di dati e una valutazione della proporzionalità tra finalità perseguite e dati raccolti, documentando le scelte adottate. La valutazione d'impatto (DPIA) è di grande ausilio tale mappatura e si rileva necessaria nella maggior parte dei casi in cui è necessario fare ricorso a BYOD. Una procedura per l'introduzione o modifica di un trattamento dovrebbe prevedere anche un approfondimento mirato in tali circostanze.

Il ruolo del DPO - Nel caso in esame noi sappiamo se, come e quali indicazioni abbia fornito il Data Protection Officer. In ogni caso le criticità sono tali che fanno immaginare che lo stesso non è stato informato o che il suo parere non è stato considerato. *.... continua a leggere online*

CONTINUA ON-LINE LA LETTURA

Fonte: Federprivacy

Dalla **COMPLIANCE** alla **GOVERNANCE**: il **DLGS 47/2026** e la trasformazione di **CYBERSECURITY**, **AI** e **PROTEZIONE** dei **DATI** negli assetti societari

> ***La cybersecurity, la protezione dei dati personali e l'AI non sono più ambiti autonomi, ma componenti di un unico sistema di governance***

L'adozione del Dlgs 27 marzo 2026, n. 47, attuativo della Legge Capitali, segna un passaggio che, pur non essendo immediatamente percepibile, è destinato a incidere profondamente sull'evoluzione della compliance digitale nelle organizzazioni. Il decreto interviene formalmente sul Testo Unico della Finanza e sulla disciplina codicistica delle società di capitali, con l'obiettivo dichiarato di rafforzare la competitività del mercato dei capitali e semplificare il quadro regolatorio. Tuttavia, al di là di tali finalità esplicite, esso contribuisce a ridefinire in modo sostanziale il ruolo della cybersecurity, dell'intelligenza artificiale e della protezione dei dati personali all'interno dell'impresa. Il dato da cui partire è negativo solo in apparenza. Il decreto non modifica la direttiva NIS2, recepita in Italia con il Dlgs 138/2024, né incide direttamente sul Regolamento Generale sulla Protezione dei Dati (GDPR). Non introduce nuovi obblighi in materia di sicurezza informatica o protezione dei dati personali, né amplia il perimetro soggettivo delle discipline esistenti. Eppure, proprio per questo motivo, il suo impatto deve essere ricercato a un livello diverso, più profondo, che attiene alla struttura stessa dell'organizzazione societaria e al modo in cui i rischi vengono governati, documentati e resi intelligibili agli organi apicali.

Il punto di svolta è rappresentato dalla riformulazione della disciplina civilistica dell'amministrazione delle società per azioni. Con il nuovo assetto delineato dall'art. 9 del decreto, agli amministratori viene attribuita in modo espresso non soltanto la gestione, ma anche l'organizzazione dell'impresa, comprensiva dell'istituzione dell'assetto organizzativo, amministrativo e contabile. Tale affermazione, che potrebbe apparire una mera precisazione sistematica, assume invece una portata dirompente se letta alla luce delle trasformazioni digitali in atto. Se l'organizzazione dell'impresa è responsabilità degli amministratori, e se la sicurezza dei sistemi informativi, la gestione dei dati personali e l'impiego di sistemi automatizzati incidono in modo diretto sul funzionamento dell'impresa stessa, ne consegue che tali ambiti non possono più essere considerati come dimensioni tecniche autonome, affidate esclusivamente a funzioni operative. La cybersecurity, in questa prospettiva, si trasforma da presidio tecnologico a componente dell'assetto organizzativo. Lo stesso vale per la protezione dei dati personali, che non può più essere ridotta a un insieme di adempimenti documentali, ma deve essere ricondotta a una logica di accountability sostanziale, coerente con quanto previsto dal GDPR. L'art. 24 del regolamento europeo impone infatti al titolare del trattamento di adottare misure tecniche e organizzative adeguate e di essere in grado di dimostrarne l'efficacia. Il Dlgs 47/2026 rafforza tale impostazione, inserendo la protezione dei dati all'interno del più ampio perimetro degli assetti societari, con la conseguenza che la dimostrazione della conformità non può più essere limitata alla produzione di documenti, ma deve emergere dai processi decisionali, dai flussi informativi e dalle strutture di controllo dell'impresa.

Un ulteriore elemento di rilievo è rappresentato dalla modifica dell'art. 123-bis del TUF, che introduce nella relazione sul governo societario l'obbligo di descrivere, ove adottate, le politiche relative all'utilizzo e al monitoraggio delle nuove tecnologie, in particolare dei sistemi di intelligenza artificiale, nonché le politiche di gestione dei rischi informatici. Tale previsione determina un passaggio significativo: la cybersecurity e l'AI governance entrano nella disclosure societaria, diventando oggetto di comunicazione verso il mercato. In questo contesto, la protezione dei dati personali assume una rilevanza ulteriore, poiché molte delle tecnologie richiamate implicano trattamenti di dati personali, talvolta su larga scala e con modalità innovative o invasive. La descrizione delle politiche aziendali in materia di tecnologie e rischi informatici non può quindi prescindere da una valutazione della conformità al GDPR, in particolare con riferimento ai principi di liceità, correttezza, trasparenza, minimizzazione e limitazione della finalità. La stessa logica si ritrova nel nuovo art. 149-ter del TUF, che disciplina i sistemi di monitoraggio continuo e gli strumenti di controllo automatici e predittivi, imponendo che essi siano adeguati e proporzionati ai rischi dell'impresa. La previsione richiama implicitamente il principio di proporzionalità, centrale tanto nella disciplina della sicurezza informatica quanto in quella della protezione dei dati personali. I sistemi di monitoraggio, spesso utilizzati per finalità di sicurezza, comportano inevitabilmente trattamenti di dati personali, talvolta relativi al comportamento degli utenti o dei dipendenti. In tali casi, la loro legittimità non può essere data per scontata, ma deve essere valutata alla luce dei principi del GDPR, eventualmente mediante una valutazione d'impatto sulla protezione dei dati. Il fatto che il legislatore societario richiami espressamente criteri di adeguatezza e proporzionalità conferma che tali strumenti devono essere governati non solo sotto il profilo tecnico, ma anche giuridico e organizzativo. Il ruolo degli organi di controllo si rafforza in modo coerente con questa evoluzione.

La vigilanza sull'adeguatezza e sul funzionamento degli assetti organizzativi implica, inevitabilmente, anche un'attenzione alla dimensione digitale. La cybersecurity e la protezione dei dati personali diventano così oggetto di verifica non soltanto da parte delle funzioni operative o di compliance, ma anche degli organi societari chiamati a garantire il corretto funzionamento dell'impresa. Ciò comporta un ampliamento del perimetro della vigilanza e una maggiore integrazione tra le diverse funzioni aziendali, con la necessità di sviluppare competenze trasversali e linguaggi comuni. In questo scenario, assume particolare rilievo il tema della supply chain. La crescente esternalizzazione di servizi tecnologici e l'utilizzo di fornitori specializzati rendono necessario un controllo più rigoroso sui soggetti terzi che trattano dati o gestiscono infrastrutture critiche. Il GDPR, attraverso l'art. 28, impone obblighi specifici nei confronti dei responsabili del trattamento, mentre la NIS2 richiede attenzione alla sicurezza della catena di approvvigionamento.

Il Dlgs 47/2026, pur non intervenendo direttamente su tali aspetti, rafforza la necessità di mantenere un controllo effettivo sulle attività esternalizzate, inserendole all'interno degli assetti organizzativi dell'impresa.

Ne deriva una responsabilità estesa, che non si esaurisce nella scelta del fornitore, ma richiede una gestione continuativa, documentata e verificabile del rapporto. Il quadro che emerge è quello di una progressiva convergenza tra discipline che, fino a pochi anni fa, venivano trattate separatamente.

La cybersecurity, la protezione dei dati personali e l'intelligenza artificiale non sono più ambiti autonomi, ma componenti di un unico sistema di governance. Il Dlgs. 47/2026 contribuisce in modo decisivo a questa evoluzione, spostando il baricentro dalla compliance tecnica alla responsabilità organizzativa e decisionale.

In tale prospettiva, il consiglio di amministrazione diventa il centro di gravità della governance digitale, chiamato a comprendere, valutare e indirizzare i rischi derivanti dalla trasformazione tecnologica. Per i professionisti della privacy, questo cambiamento implica una revisione del proprio ruolo. Non si tratta più soltanto di garantire la conformità al GDPR, ma di contribuire alla costruzione di assetti organizzativi integrati, in cui la protezione dei dati sia parte integrante dei processi decisionali e dei sistemi di controllo. In conclusione, il Dlgs 47/2026, pur non essendo una norma di cybersecurity o di protezione dei dati personali, rappresenta un tassello fondamentale nel processo di evoluzione della governance digitale.

Esso contribuisce a definire un modello in cui la gestione dei rischi informatici e la tutela dei dati personali non sono più attività accessorie, ma elementi essenziali dell'organizzazione dell'impresa. La sfida che si apre è culturale prima ancora che normativa: si tratta di superare la logica della compliance frammentata per approdare a una visione integrata, in cui diritto societario, cybersecurity e protezione dei dati convergano in un unico sistema di responsabilità e controllo.

Francesco Capparelli
Chief Cybersecurity Advisor
di ICT Cyber Consulting

SCOPERTA nuova **MINACCIA "ZERO-CLICK" su WHATSAPP**: per clonarvi l'account agli hacker basta mandarvi un messaggio senza bisogno di cliccare su alcun link

> Gli insidiosi **attacchi "zero-click" su WhatsApp** infettano lo smartphone alla mera ricezione di un file, senza alcuna interazione dell'utente

Un nuovo allarme legato a WhatsApp sta preoccupando gli esperti di cybersicurezza: si tratta degli attacchi "zero-click", una tipologia di minaccia informatica particolarmente insidiosa perché può colpire gli utenti senza richiedere alcuna azione da parte loro.
Non è necessario aprire link sospetti, scaricare allegati o interagire con messaggi apparentemente anomali. In alcuni casi, infatti, può bastare la semplice ricezione di un contenuto per esporre il dispositivo a un tentativo di compromissione. Secondo quanto riportato da Fanpage, questo genere di attacco sfrutta vulnerabilità presenti nei sistemi di gestione dei messaggi delle applicazioni di messaggistica.
Gli hacker inviano contenuti creati appositamente per aggirare i controlli di sicurezza dell'applicazione e attivare automaticamente codice malevolo sul dispositivo della vittima. L'operazione avviene in modo silenzioso e spesso senza segnali evidenti, rendendo molto difficile accorgersi immediatamente della compromissione.
Tra i rischi più rilevanti associati a questi attacchi figurano l'accesso ai messaggi privati, il furto di dati personali e, nei casi più gravi, la clonazione dell'account. Proprio l'assenza di interazione richiesta agli utenti rappresenta l'elemento che preoccupa maggiormente gli specialisti del settore: le tradizionali raccomandazioni basate sull'attenzione ai link sospetti o agli allegati malevoli non sempre sono sufficienti contro vulnerabilità di questo tipo.
Gli attacchi zero-click vengono considerati tra le tecniche più sofisticate nel panorama della cybersecurity. Spesso sfruttano falle "zero-day", cioè ulnerabilità non ancora corrette dagli sviluppatori o individuate solo di recente.
In questi scenari, il malware può attivarsi automaticamente durante l'elaborazione dei contenuti ricevuti dall'applicazione, senza che gli utenti compiano alcuna operazione.
Secondo le analisi degli esperti, anche i file multimediali possono trasformarsi in vettori di attacco. Immagini, video o documenti apparentemente innocui potrebbero contenere codice predisposto per sfruttare bug presenti nelle applicazioni o nei sistemi operativi. In alcune circostanze, il semplice download automatico dei contenuti può facilitare la diffusione di software malevoli.
Per ridurre i rischi, gli specialisti consigliano di mantenere sempre aggiornati WhatsApp e il sistema operativo dello smartphone, installare tempestivamente le patch di sicurezza e attivare l'autenticazione a due fattori. Viene inoltre suggerito di controllare periodicamente i dispositivi collegati all'account e prestare attenzione a eventuali comportamenti anomali dell'applicazione, come accessi non riconosciuti o messaggi già visualizzati senza motivo apparente.
L'episodio conferma come il panorama delle minacce informatiche stia diventando sempre più sofisticato, e le applicazioni di messaggistica istantanea utilizzate ogni giorno da miliardi di persone rappresentano obiettivi particolarmente appetibili per i cybercriminali, soprattutto quando vulnerabilità invisibili agli utenti consentono attacchi difficili da individuare e ancora più complessi da prevenire.

LEGGI ON-LINE

Fonte: Fanpage

MC3 INNOVATION
ORGANIZZAZIONE - QUALITÀ - PRIVACY

L'Architettura Digitale della tua Compliance

Integriamo Consulenza Specialistica e Soluzioni Software per trasformare gli obblighi normativi in efficienza operativa.

CONSULENZA STRATEGICA

Data Protection & Privacy
Assunzione del ruolo di DPO Esterno, redazione registri del trattamento, DPIA e gestione della sicurezza dei dati.

Modelli Organizzativi 231
Progettazione, implementazione e supporto all'Organismo di Vigilanza (OdV) per la prevenzione dei reati amministrativi.

Ottimizzazione e gestione dei processi aziendali
analisi e mappatura dei processi, misurazione delle performance (KPI), ottimizzazione e Riprogettazione (BPR)

Formazione Avanzata
Piani formativi su misura per dipendenti e consulenti, anche tramite piattaforme e-learning.

SOLUZIONI SOFTWARE

Gestione documentale & workflow
automatizziamo i flussi approvativi e la conservazione digitale per eliminare l'errore umano con l'AI a supporto della gestione documentale

Software per la compliance
Tool dedicati per la gestione del Whistleblowing, dell'analisi dei rischi e del monitoraggio dei KPI di conformità.

Piattaforme di Governance
Sistemi integrati per mappare processi, scadenze e adempimenti in tempo reale, garantendo la piena Accountability.

Richiedi il tuo Compliance Check-up gratuito:
scrivi a **info@mc3innovation.it** citando '***Federprivacy***',
oppure inquadra il Qrcode qui

MC3 INNOVATION
ORGANIZZAZIONE - QUALITÀ - PRIVACY

Consulenza specialistica e soluzioni digitali per trasformare la compliance in efficienza.
Data Protection, Modelli 231 e Sistemi di Gestione in un unico ecosistema di sicurezza, legalità e innovazione.

Via Trieste 14, 27029 Vigevano (PV)

info@mc3innovation.it 0381 691010 www.mc3innovation.it

Per molte **STARTUP** la **PRIVACY** diventa un **TEMA STRATEGICO** quando è **TROPPO TARDI**

> ***Non si tratta di trasformare una startup in una corporate ossessionata dalla compliance ma di trattare il dato come un asset, non come un sottoprodotto***

Nelle prime fasi di vita di una startup la privacy è quasi sempre una questione secondaria. Non viene ignorata, ma raramente è una priorità. Il focus è sul prodotto, sulla crescita, sull'acquisizione utenti. La compliance? Verrà dopo. Il problema è che quel "dopo" non arriva mai in modo graduale. Arriva tutto insieme. E spesso nel momento peggiore possibile.

La privacy diventa centrale quando la startup entra in una fase finanziaria matura: un round strutturato, una trattativa con un fondo, una possibile acquisizione, l'ingresso di un cliente enterprise. È in quel momento che qualcuno inizia a fare le domande giuste. Come sono stati raccolti i dati? Su quale base giuridica? Con quali informative? Per quanto tempo vengono conservati? Esistono trasferimenti extra UE? Chi ha accesso ai database? Ed è lì che molte startup scoprono che la crescita è andata più veloce della governance.

Il problema non sono le sanzioni - Contrariamente a quanto si pensa, raramente un'operazione salta per il timore immediato di una sanzione ai sensi del Regolamento generale sulla protezione dei dati. Le multe fanno rumore nei convegni, molto meno nei tavoli di investimento. Il vero problema è l'incertezza.

Se non è chiaro su quali basi giuridiche siano stati trattati i dati, se le informative sono lacunose o incoerenti, se i consensi sono generici o non tracciabili, se non esiste una policy di data retention, quell'incertezza si trasforma in rischio contrattuale. E il rischio, nel linguaggio del business, ha sempre un prezzo. Il GDPR non è solo una norma sanzionatoria. È un framework di accountability. E quando manca la tracciabilità delle scelte, ciò che viene meno non è solo la compliance: viene meno la difendibilità dell'asset.

Quando la due diligence fa emergere la zona grigia - Immaginiamo una startup SaaS che in cinque anni costruisce una piattaforma con centinaia di migliaia di utenti registrati. Modello freemium, crescita trainata dal marketing digitale, analisi comportamentale in-app, dataset ricco e segmentato. Arriva un fondo internazionale interessato a un'acquisizione strategica. I numeri sono solidi: ARR in crescita, churn sotto controllo, metriche di engagement convincenti.

Durante la due diligence emerge però un dettaglio:

– le informative privacy sono state aggiornate più volte senza conservare le versioni precedenti;

– i consensi marketing sono stati raccolti con formule generiche;

– alcune attività di profilazione sono state giustificate alternativamente come consenso o legittimo interesse;

– non esiste una politica chiara di conservazione: i dati di utenti inattivi da anni sono ancora tutti nei database.

Non c'è una violazione evidente. Non ci sono indagini in corso. Ma c'è una zona grigia.

Il fondo non si ritira. Chiede però garanzie rafforzate, una revisione completa dei flussi di trattamento prima del closing e accantona una parte del prezzo in escrow per coprire eventuali rischi futuri.

La valutazione viene rivista al ribasso per tenere conto del costo della remediation e dell'incertezza sull'effettiva utilizzabilità di alcuni dataset. La startup non perde l'exit. Perde valore.

Il dato come asset fragile - Il problema nasce quasi sempre all'inizio del percorso. Informative copiate da un competitor. Consensi raccolti "per sicurezza". Basi giuridiche sovrapposte. Dati accumulati nel tempo senza una logica di minimizzazione. Scelte comprensibili, prese quando il team era composto da poche persone e l'obiettivo era crescere rapidamente.

Ma quelle decisioni producono un effetto preciso: trasformano il dato in un asset fragile. Nel mondo startup si parla continuamente di traction, retention, ARR, churn. Molto meno della qualità del dato sotto il profilo giuridico. Eppure, per chi investe o acquisisce, la domanda è sorprendentemente semplice: questi dati potrò usarli domani senza problemi?

Se la risposta non è chiaramente positiva, il valore dell'asset si ridimensiona.

Non per formalismo, ma per gestione del rischio. Il GDPR impone principi chiari: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, conservazione proporzionata. Non sono clausole astratte. Sono criteri di valutazione economica quando il dato diventa parte della valuation.

Il momento in cui la privacy cambia natura - Nelle fasi early stage nessuno guarda davvero la privacy in profondità. Finché i numeri sono piccoli, il rischio appare teorico. Poi la startup cresce, aumenta il volume dei dati, aumenta la visibilità, aumentano gli stakeholder coinvolti. A quel punto la privacy smette di essere un tema operativo e diventa un tema strategico.

Non si tratta di trasformare una startup in una corporate ossessionata dalla compliance. Si tratta di fare scelte coerenti e difendibili. Di sapere spiegare cosa si è fatto, perché si è fatto e su quali basi giuridiche. In altre parole: trattare il dato come un asset, non come un sottoprodotto.

La verità che pochi founder vogliono sentire - La privacy difficilmente distrugge una startup. Ma può ridurre drasticamente il valore del suo successo. E scoprirlo quando il term sheet è già sul tavolo è uno dei modi peggiori per impararlo.

Fonte: Startupitalia
Articolo di Teresa Fontana, Avvocato d'impresa per PMI e startup

opera
professioni

PRIVACY

WHISTLEBLOWING

ANTICORRUZIONE

TRASPARENZA

ANTIRICICLAGGIO

MODELLI 231

operaprofessioni.it

mail: info@operaprofessioni.it
tel: +39 080 8406912
web: operaprofessioni.it

Via Antichi Pastifici, 17
70056 Molfetta (BA)

Str. del Portone, 159
10095 Grugliasco (TO)

Anche **UN TERZO** può **IMPUGNARE** il **SEQUESTRO** dello **SMARTPHONE CONTENENTE DATI SENSIBILI**

> Con **due sentenze**, la **n. 15010/2026** e la **n. 15894/2026**, la Cassazione fa chiarezza sulla legittimazione a impugnare il provvedimento di sequestro del telefonino

Anche chi non è proprietario dello smartphone può presentare opposizione al sequestro da parte dell'autorità giudiziaria. Tuttavia il luogo comune che del telefono cellulare fa il deposito di segmenti importanti della vita del proprietario non legittima di per sè stesso l'impugnazione.

Con due distinte e recenti sentenze, la n. 15010/2026 e la n. 15894/2026 entrambe della Terza sezione, la Cassazione fa chiarezza sulla legittimazione a impugnare il provvedimento di sequestro del telefonino.

Opposizione all'acquisizione delle prove - Con la prima pronuncia, la Cassazione sottolinea come nel caso di sequestro probatorio di un bene, come un telefono cellulare, l'interesse di chi propone impugnazione non risiede solamente della rimozione del vincolo reale, con conseguente restituzione del bene stesso, ma anche nell'opporsi all'acquisizione di elementi di prova, da esso estraibili, come i dati contenuti nel telefono cellulare utilizzabili, a carico del ricorrente, nel processo di merito.

Il dato essenziale è costituito, così, per la Corte, dal fatto che chi impugna aspira al dissequestro, come esito da cui discende, anche per lui, una concreta utilità, anche nella forma di eliminazione di un pregiudizio, riferibile «a una situazione giuridica soggettiva tutelata e riconosciuta dall'ordinamento e non solo valutata soggettivamente come tale in via di fatto, magari in relazione a una gamma di situazioni coinvolgenti rapporti familiari, affettivi ed economici collaterali, che non diano luogo a specifiche riconoscibili posizioni giuridiche direttamente incise dal vincolo di indisponibilità».

Ammissibile allora l'impugnazione da parte dei coindagati perché, come emerge dallo stesso decreto di sequestro, il telefono è stato considerato elemento di prova indispensabile per l'accertamento fatti, nel confermare l'identificazione di alcuni indagati e metterne in evidenza il ruolo in un contesto di associazione criminale.

Sequestro e dati sensibili - Con la seconda sentenza, la Cassazione mette in evidenza come il titolare di dati sensibili contenuti in documenti informatici o telematici che intende contestare un provvedimento di sequestro è sempre obbligato ad allegare all'impugnazione l'interesse concreto e attuale alla loro disponibilità esclusiva. Ritenere, afferma la Corte, che in caso di sequestro di uno strumento informatico, destinato per la sua stessa natura a raccogliere dati informatici di natura personale e professionale (e la sentenza esemplifica in materiale audiovisivo, dati di localizzazione, posta elettronica, password, dati relativi al traffico telefonico, messaggistica) a giustificare l'impugnazione basti la sottolineatura della natura dello strumento e della altrettanto naturale e generica presenza dei dati stessi al suo interno e quindi della ovvia esistenza di un interesse sarebbe eccessivo.

Per la Cassazione, infatti, la conseguenza sarebbe quella di obbligare il pubblico ministero, per la legittimità stessa del provvedimento, a un vincolo di motivazione tanto stringente da essere poi nei fatti inesigibile, con un'eccessiva compressione dell'attività d'indagine. Infatti, va ricordata la «peculiare connotazione dei documenti informatici, che, nella generalità dei casi, richiedono, sia in ragione del loro contenuto, spesso promiscuo, che della loro mole, accertamenti tecnici per estrapolarne e selezionare quanto utile alle indagini».

APPROFONDIMENTO GRATUITO PER GLI UTENTI DEL SITO FEDERPRIVACY

Fonte: Il Sole 24 Ore – Articolo di Giovanni Negri

UTOPIA

Rispetta gli obblighi e dimostra la tua accountability

UTOPIA è il software efficace e completo per migliorare il tuo sistema di gestione privacy.

Dedicato a consulenti, PMI, grandi aziende, gruppi e pubbliche amministrazioni.

✓ **Prova gratuita** ✓ **Utenti illimitati** ✓ **Cloud certificato**

Massima personalizzazione

Crea cataloghi personalizzati o scegli tra quelli disponibili, realizza questionari, modifica i modelli di documento, importa ed esporta ogni dato.

Abbonamenti su misura

Scegli il piano più adatto tra diverse tipologie di abbonamento pensate per consulenti, PMI, grandi aziende e pubbliche amministrazioni.

Supporto specializzato

Contatta il nostro team direttamente dal tuo account, puoi parlare con un esperto, risolvere dubbi, chiedere consigli o proporre nuove funzionalità.

Aggiornamenti continui

UTOPIA si evolve costantemente con nuove funzionalità e miglioramenti periodici garantendoti uno strumento sempre aggiornato e completo.

+10.000	+8.000	+70.000	+75.000
organizzazioni gestite	utenti creati	trattamenti inseriti	persone autorizzate

Powered by

Hubenture
SOFTWARE AS EXPERIENCE

In collaborazione con

STUDIOLEGALEPRIVACY BY ORLANDI&PARTNERS

www.utopiathesoftware.com

MERCATO CRIMINALE DELLE INFORMAZIONI: piaga sociale o fallimento dello Stato?

> Il **furto di dati personali**, le **violazioni dei dati**, il **furto di identità** e la circolazione di dossier informativi dimostrano come il valore insito nelle informazioni renda tali **contenuti molto appetibili per chi mira a ottenere vantaggi economici o strategici**

I recenti accadimenti giudiziari di cui ha riferito la Procura di Napoli riguardanti il mercato criminale delle informazioni – che vedono coinvolti imprenditori, investigatori privati, forze dell'ordine e dipendenti di INPS ed Agenzia delle Entrate – oltre a evidenziare il malcostume della corruzione, pongono nuovamente all'attenzione il profondo cambiamento dell'informazione nell'odierna società digitale.

Quella che in passato fungeva principalmente da mezzo di trasmissione, si è progressivamente trasformata in una risorsa fondamentale dal valore economico, politico e sociale sempre più significativo. La conversione dei processi produttivi e amministrativi in formati digitali ha reso possibile la raccolta di enormi volumi di dati, strutturando un contesto in cui l'informazione assume un ruolo centrale nelle dinamiche di potere. Le entità che operano in ambito digitale traggono il proprio vantaggio competitivo proprio dalla capacità di accumulare e interpretare i dati, trasformando il possesso di informazioni in una vera e propria infrastruttura in grado di plasmare l'equilibrio dei mercati. Tuttavia, l'importanza strategica delle informazioni ha dato origine a nuove categorie di esposizione. La sfera digitale vede una trasmissione continua di dati tra piattaforme e utenti, spesso senza la piena consapevolezza dei rischi.

Questo stato di cose facilita il furto, la manomissione o l'uso improprio dei dati, alimentando un mercato criminale che trae profitto dal loro sfruttamento. Il fenomeno dimostra come il valore insito nelle informazioni renda tali contenuti appetibili per chi mira a ottenere vantaggi strategici.

Per i non addetti ai lavori può essere sorprendente come i dati possano abbandonare il loro ruolo iniziale per trasformarsi in uno strumento di coercizione e pressione in grado di influenzare decisioni giudiziarie e politiche, orientare l'opinione pubblica o destabilizzare i rapporti istituzionali.

L'avvento di questi rischi ha reso necessaria l'evoluzione di meccanismi normativi sempre più complessi, come le politiche di sicurezza informatica, le direttive europee e le leggi nazionali sulla sicurezza digitale.

Tali misure denotano una crescente consapevolezza da parte delle autorità, ma il rapido ritmo dell'evoluzione tecnologica complica la garanzia di una protezione totale. Le debolezze tecniche, unite a fattori umani e organizzativi, continuano a rappresentare punti critici. Spesso la compromissione dei dati non deriva da sofisticate intrusioni, ma da errori degli utenti, configurazioni inadeguate o compravendite illegali. La sicurezza non può quindi essere affidata solo a soluzioni tecniche o legislative: serve una metodologia integrata che coinvolga istituzioni e imprese nella promozione di una cultura della consapevolezza.

In una società basata sui dati, la capacità di salvaguardare le informazioni diventa un prerequisito per mantenere la fiducia e la stabilità economica e istituzionale.

La traiettoria del crimine informatico conferma che le informazioni sono ormai una risorsa strategica centrale dell'era digitale. Nonostante gli sforzi, la vicenda di Napoli dimostra però come quello stesso Stato che pretende di sapere tutto di noi, non predisponga sufficienti misure di sicurezza a presidio dei nostri dati, evidenziando l'insufficienza delle tutele a protezione di quelle informazioni che ci obbliga a fornirgli.

LEGGI ON-LINE

Fonte: Articolo di Andrea Pedicone, consulente investigativo ed in materia di protezione dei dati personali

CYBER-GOVERNANCE e **COMPLIANCE** nella **SUPPLY-CHAIN**, il **GDPR** come best practice

> Una **best practice** è il GDPR quando in sede di individuazione di un potenziale Responsabile Esterno, richiede preventivamente di valutarne le **«garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate»** al trattamento dei dati

CONTINUA ON-LINE LA LETTURA

La moderna "Data Governance" – in particolar modo alla luce di quel normale processo evolutivo di innovazione tecnologica, che ha portato a quella che comunemente viene definita "Artificial Intelligence" - non dovrebbe essere vista come un mero adempimento di compliance alle normative e regolamenti emanati negli ultimi 10 anni (a mero titolo esemplificativo e non esaustivo: GDPR, la NIS2, DORA, Data Act, etc.). Il tutto dovrebbe essere letto ed interpretato nel contesto di quella UE Digital Agenda che vuole essere non una imposizione di obblighi, bensì un atto di responsabilità politica e di governo, che ha la finalità elevata di consentire di vedere - a tutti i livelli - la visione sui possibili scenari che si stanno venendo a creare, nella interazione tra assetti geopolitici, possibilità tecnologiche, interessi economici, e mutamento (anche culturale) delle diverse comunità sociali locali. Sebbene non sia espressamente dichiarato, l'osservatore attento, può intravedere una corretta applicazione di quel "G-Local" di Baumann, che è chiave di lettura dei moderni fenomeni. Invero il quadro legislativo degli ultimi anni, è caratterizzato da interventi regolatori basati sulla visione strategica multilivello: pone l'attenzione (nella logica dell'approccio basato sul rischio) sulla preventiva risposta ad ipotetici ed attesi (expected) eventi negativi: tematica complessa, di cui gli attori - pubblici e privati, ossia pubblica amministrazione, aziende e cittadini - sono de facto poco consapevoli. Pertanto, il significato di fondo dell'azione dell'UE è di sensibilizzare e di rafforzare la consapevolezza (digital awareness), sui nuovi fenomeni tecnologici e geopolitici, al fine di poter prevenire ed evitare i potenziali effetti distorsivi, in specie di natura sistemica. Anche per le precedenti considerazioni, dal punto di vista tecnico (e lessicale) si dovrebbe fare – più opportunamente - riferimento alla Digital Governance (secondo la definizione data dal legislatore Europeo), che ricomprende contestualmente dati e infrastruttura, ossia componente tangibile ed intangibile. Anche se in effetti, sarebbe anche possibile sostituire il primo termine con "cyber", visto che si richiama e si conferma il riferimento ad una dimensione ibrida, senza alcuna soluzione di continuità.

Una chiosa - Quotidianamente, ciascuno di noi genera, elabora e processa una molteplicità di dati (personali e non; sintetici; impersonali; etc.) e metadati, senza soffermarsi su alcune considerazioni (apparentemente) "banali". Lo strumento utilizzato (device) su cui li "trattiamo" è uno solo; i processi di trattamento avvengono tanto "stand alone", quanto su complesse supply chain (basti pensare ai cloud); ciascun device è ormai AI-based , al di la della effettiva consapevolezza del singolo interessato, utente, provider. A fronte di un tale scenario senza compartimenti stagni, al contrario, le normative sono verticali su singoli aspetti.

Per cui, se da un lato aziendale è necessario adottare una visione/approccio olistico-complesso ; dall'altro, ben venga la scelta del legislatore UE di armonizzare le diverse norme. Dal costo all'investimento - Purtroppo, si rileva come la declinazione della "compliance" si sia ridotta ad un inadeguato approccio (spesso) "formalistico" e non sostanziale: sovente demandato ad una serie di check list elaborate a fronte delle singole richieste normative, traducendo il tutto in un inutile e gravoso costo aziendale, senza alcun output funzionale e di interesse. Al contrario, occorrerebbe adottare una visione gestionale (per l'appunto di Governance strategica) per cui si procede con un investimento per irrobustire la componente tecnologica (infrastruttura e software) a presidio nonché di cybersecurity dell'asset immateriale, oggigiorno, più significativo: il dato (personale e non).

.... continua a leggere online

Fonte: Articolo di Manlio d'Agostino Panebianco, Membro del Comitato Scientifico di Federprivacy

NEOSTUDIO CONSULENZA E RISK MANAGEMENT

Il Gruppo Neostudio, con il suo team composto da Giuristi, Commercialisti, Informatici e Riskmanager, opera da oltre 20 anni là dove si incontrano business, organizzazione e norme.

Rendiamo conformi alle norme ed efficienti le aziende

Lavoriamo insieme alle aziende clienti per guidarle in un percorso che coniuga efficienza e protezione giuridica, con interventi mirati in base al settore di attività, alla dimensione e alla capacità aziendale su conformità al GDPR e AI Act e redazione e start-up all'efficace attuazione sui modelli di organizzazione in conformità al D.Lgs. 231/01.

L'importanza dei dati personali

Creiamo un vero e proprio modello organizzativo GDPR, conforme alle linee guida e alle norme tecniche rilevanti, nel quale il Registro dei Trattamenti diventa un cruscotto di monitoraggio e controllo, nonché il cuore dei documenti da mettere a disposizione dell'Autorità Garante. Nei progetti ad alto valore tecnologico che prevedano, ad esempio, l'utilizzo di algoritmi di intelligenza artificiale ed LLM, lo specifico assessment previsto dal GDPR viene integrato con le ulteriori valutazioni di impatto previste dalle specifiche norme in materia, come ad esempio l'AI Act. Supportiamo dunque le aziende, ed in particolare gli implementatori (c.d. deployer, ai quali compete la necessità di motivare la scelta di una determinata tecnologia) nella conduzione dell'Artificial Intelligence Impact Assessment e del Fundamental Rights Impact Assessment, in modo integrato ed efficiente, producendo la relativa documentazione a supporto delle scelte tecnologiche ed operative effettuate.

L'importanza della Ricerca

Il nostro coinvolgimento in attività istituzionali e di Ricerca e docenza in ambito universitario ci permette di essere in prima linea a fronte delle più recenti novità normative e giurisprudenziali, orientandone le ricadute concrete sulle attività aziendali: ultimi esempi sono progetti e servizi che affrontano la sempre maggiore convergenza. tra Antitrust e Data Protection (con il trattamento illecito di dati personali interpretato anche come concorrenza sleale), nonché tra Modelli 231, strumenti di compliance fiscale e la virtuosa relazione che questo ha con i fattori della compliance ESG.

Neostudio S.r.l.
Via Luigi Settembrini, 18
50133 Firenze
Tel: 0550106651

Neo Governance | Associazione Tra Professionisti
Via Carducci, 34
20123 Milano
Tel: 0237920149

Neo Studio 2000 S.r.l.
Largo Villaura, 27
90142 Palermo
Tel: 091 36 49 24

neostudio.it
neostudio@neostudio.it

NEOSTUDIO
MODELLI, ORGANIZZAZIONE, PROTEZIONE DEI DATI.

AUTOVELOX sempre più intelligenti, ma **AMMINISTRAZIONI LOCALI** poco rispettose della **PRIVACY** degli **AUTOMOBILISTI**

Per una **digitalizzazione pubblica efficiente non servono controlli indiscriminati**, **ma una governance virtuosa** che bilanci legalità e privacy, scongiurando il rischio di una opprimente società del controllo

LEGGI ON-LINE

Specialmente con la diffusione delle nuove tecnologie, le multe stradali sono ormai diventate una miniera d'oro per le casse di molti Comuni italiani, che sono sempre pronti a sanzionare automobilisti e motociclisti che infrangono le regole del Codice della Strada, ma a quanto pare le stesse amministrazioni locali non sono altrettanto ligie nel rispettare le normative vigenti, comprese quelle in materia di privacy. Le elaborazioni sui dati Siope (Sistema informativo sulle operazioni degli enti pubblici) relative allo scorso anno evidenziano infatti che gli incassi delle sanzioni per violazioni del Codice della Strada hanno raggiunto un vero e proprio tesoretto di circa 1,9 miliardi di euro, ma d'altro canto i dati diffusi nel marzo 2026 dal Ministero delle Infrastrutture e dei Trasporti rivelano che dei circa 11.000 dispositivi di controllo delle infrazioni stradali che risultano individuati sul territorio nazionale, sono solo 3.900 quelli regolarmente registrati nella piattaforma telematica gestita dal Mit per il censimento dei dispositivi di rilevamento della velocità, e solo il 29% delle apparecchiature risulta compatibile con i requisiti di omologazione richiesti dalla normativa. Secondo il Codacons, il 59,4% degli autovelox fissi e il 67,2% di quelli mobili presenti nelle principali città italiane risulterebbero infatti privi di una omologazione pienamente conforme ai requisiti indicati dalla giurisprudenza. Eppure, la marea di multe che inonda il Belpaese non concede tregua agli automobilisti, nonostante diverse pronunce della Corte di Cassazione abbiano ribadito che, ai fini della validità delle sanzioni, il Codice della Strada richiede espressamente che le infrazioni possano essere accertate solo attraverso dispositivi regolarmente omologati, e non solo "approvati" dal Ministero delle Infrastrutture e dei Trasporti. E se in passato dispositivi automatici come gli autovelox si limitavano a rilevare il superamento dei limiti di velocità, adesso le nuove tecnologie e l'intelligenza artificiale sono molto più pervasive e consentono alle forze dell'ordine di scrutare ogni dettaglio all'interno dell'abitacolo, verificando in tempo reale se il conducente parla al telefono senza vivavoce o sbircia i messaggi sul display dello smartphone, se ha le cinture allacciate, se accede a una Ztl senza autorizzazione, ma anche se il veicolo ha la copertura assicurativa, se è rubato o sottoposto a fermi amministrativi, se ha la revisione scaduta, la sua classe inquinante, e perfino se risulta in qualche black list o white List. È vero che è giusto che chi trasgredisce debba pagarne le conseguenze, e che è doveroso preservare il controllo della legalità sul territorio, ma se in uno Stato di diritto la legge è davvero uguale per tutti, anche le istituzioni che infliggono le multe dovrebbero rispettare le regole, specialmente se gli occhi elettronici arrivano a fare praticamente i "raggi x" a conducenti e veicoli in modo massivo e talmente accurato da non concedere il minimo sgarro. A dimostrare come molte amministrazioni locali non diano il buon esempio nel rispettare le leggi, è l'ennesimo intervento in cui il Garante per la protezione dei dati personali ha sanzionato un comune per violazione del Gdpr.

Nel paradossale caso in questione, a violare la privacy dei cittadini era infatti la polizia municipale, che si avvaleva di un sistema di videosorveglianza per incrociare i dati della Motorizzazione Civile con quelli delle targhe dei veicoli che transitavano per la strada con lo scopo di scovare quelli con la revisione scaduta.

Peccato che, oltre a non essere regolarmente omologato, lo strumento non rispettasse neanche le basilari regole prescritte dalla normativa per informare in modo trasparente gli automobilisti con appositi cartelli su quali fossero le modalità e le basi giuridiche utilizzate per effettuare le video rilevazioni, senza neppure specificare quali fossero i loro diritti e a chi rivolgersi per esercitarli.

Per una trasformazione digitale della pubblica amministrazione efficiente e sostenibile non basta quindi investire in tecnologia per fare cassa o aumentare i controlli in modo indiscriminato. Occorre invece una virtuosa governance per presidiare la legalità e tutelare anche la privacy dei cittadini per scongiurare il rischio di creare una oppressiva società del controllo in cui nessuno vorrebbe vivere. E gli enti che esercitano il proprio potere per far rispettare le regole, hanno anche il dovere di essere i primi a rispettarle.

Fonte: Economy – Articolo di Nicola Bernardi, Presidente di Federprivacy

Garante Privacy agli albergatori: no alla conservazione di copia dei documenti d'identità degli ospiti

Alberghi, B&B e affittacamere non possono conservare copie dei documenti d'identità degli ospiti oltre il tempo strettamente necessario alla comunicazione dei dati alle autorità di pubblica sicurezza. Lo chiarisce il Garante per la protezione dei dati personali in una nota inviata alle associazioni di categoria del settore, anche alla luce dell'aumento di segnalazioni e violazioni dei dati personali registrate negli ultimi mesi. La normativa vigente impone ai gestori delle strutture ricettive di identificare i clienti e di trasmettere i relativi dati alle autorità di pubblica sicurezza tramite il portale "Alloggiati Web". Tale obbligo, tuttavia, non legittima la conservazione, da parte delle strutture, di fotocopie o immagini dei documenti d'identità. Negli ultimi tempi si è diffusa, soprattutto tra B&B e affittacamere, la pratica di fotografare i documenti con smartphone o di richiederne l'invio tramite applicazioni di messaggistica, come WhatsApp. Comportamenti che, sottolinea il Garante, espongono ingiustificatamente gli interessati a rischi concreti, tra cui furti d'identità e accessi illeciti ai dati personali. L'Autorità ribadisce che, come previsto da un obbligo normativo, una volta completata la trasmissione dei dati alle autorità di pubblica sicurezza, eventuali copie dei documenti acquisite per tale finalità devono essere immediatamente cancellate o distrutte. L'unico elemento che può essere conservato è la ricevuta dell'avvenuta comunicazione, prodotta automaticamente dal portale, da conservare per cinque anni al fine di comprovare l'adempimento. Il Garante sottolinea, inoltre, che è preciso dovere dei titolari del trattamento garantire la sicurezza dei dati personali. Le strutture ricettive devono quindi adottare misure adeguate per la protezione dei dati e istruire correttamente il personale incaricato della loro raccolta e gestione. È stato ricordato, infine, che in caso di violazione dei dati personali - data breach - scattano obblighi specifici, tra cui la notifica al Garante entro 72 ore e, nei casi più gravi, anche la comunicazione della violazione agli interessati. Le associazioni di categoria sono state invitate a diffondere tra i propri iscritti le indicazioni dell'Autorità, tenuto conto che l'attività ricettiva comporta ogni anno il trattamento dei dati personali di milioni di persone.
Fonte: Garante Privacy

La scure del Garante Privacy colpisce ancora Intesa Sanpaolo: sanzione da 31,8 milioni di euro per misure di sicurezza inadeguate

A distanza di appena pochi giorni dalla sanzione di 17,6 milioni di euro per il trasferimento dei dati di 2,4 milioni di clienti alla controllata al 100% Isybank Spa, Intesa Sanpaolo finisce ancora sotto la scure del Garante Privacy con una seconda sanzione di 31,8 milioni di euro, stavolta per gravi carenze nella sicurezza dei dati personali, dovute all'inadeguatezza delle misure tecniche e organizzative adottate. L'istruttoria dell'Autorità – avviata a seguito del data breach notificato dalla banca nel luglio 2024 – ha accertato che un dipendente ha avuto accesso, senza giustificato motivo, alle informazioni bancarie di 3.573 clienti, effettuando oltre 6.600 consultazioni tra il 21 febbraio 2022 e il 24 aprile 2024. Tali accessi indebiti non sono stati rilevati dai sistemi di controllo interni, evidenziando significative criticità nei meccanismi di monitoraggio e prevenzione. L'accesso illecito ha riguardato anche dati relativi a clienti "ad alto rischio", tra cui soggetti con ruoli di rilievo pubblico, per i quali sarebbero stati necessari presidi di controllo rafforzati. L'Autorità ha accertato, in particolare, la violazione dei principi di integrità e riservatezza dei dati personali, nonché del principio di accountability, rilevando l'inadeguatezza complessiva delle misure adottate. Il modello operativo utilizzato, che consentiva agli operatori di interrogare in piena circolarità l'intera base clienti, non era infatti adeguatamente bilanciato da controlli idonei a prevenire e individuare accessi non giustificati. Ulteriori criticità sono emerse nella gestione del data breach. La notifica è risultata incompleta e tardiva rispetto ai termini previsti dalla normativa, così come la comunicazione agli interessati, avvenuta solo a seguito di un precedente provvedimento del Garante del 2 novembre 2024 (doc. web n. 10070521). Tali condotte hanno compromesso la possibilità di un tempestivo intervento dell'Autorità a tutela dei diritti e delle libertà delle persone coinvolte. Alla luce delle violazioni riscontrate, il Garante ha ritenuto illecita la condotta posta in essere da Intesa Sanpaolo. Nel determinare l'importo della sanzione, l'Autorità ha tenuto conto della gravità e della durata delle violazioni, dell'elevato numero di clienti coinvolti, nonché delle misure correttive adottate dall'istituto successivamente ai fatti, finalizzate al rafforzamento dei sistemi di controllo interno e dei presidi di sicurezza. Con questo secondo provvedimento, l'ammontare delle sanzioni inflitte dal Garante a Intesa Sanpaolo sale quindi a 49,4 milioni di euro nell'arco di pochi giorni.
Fonte: Garante Privacy

Il Garante Privacy sanziona Poste italiane e Postepay per oltre 12,5 milioni di euro. La replica: "Stupiti del provvedimento, presenteremo ricorso"

IIII Garante per la protezione dei dati personali ha irrogato una sanzione di 6.624.000 euro a Poste Italiane S.p.A. e una di 5.877.000 euro a Postepay S.p.A., per aver trattato illecitamente i dati personali di milioni di utenti. L'istruttoria dell'Autorità – avviata a seguito di numerose segnalazioni e reclami pervenuti a partire da aprile 2024 – ha riguardato, in particolare, le modalità di funzionamento delle app BancoPosta e Postepay. Tali applicazioni prevedevano, quale condizione obbligatoria per l'utilizzo dei servizi, il rilascio da parte degli utenti di un'autorizzazione al monitoraggio di una serie di dati contenuti nei dispositivi mobili, incluse le applicazioni installate e in esecuzione, al fine di individuare eventuali software malevoli. Secondo quanto dichiarato dalle società, tali trattamenti sarebbero stati necessari per garantire la sicurezza delle operazioni e conformarsi alla normativa in materia di servizi di pagamento. Il Garante ha tuttavia rilevato che le modalità adottate comportavano un'ingerenza eccessivamente invasiva nella sfera privata degli utenti, in quanto non risultavano strettamente necessarie rispetto alle finalità di prevenzione delle frodi. Nel corso dell'istruttoria sono inoltre emerse diverse violazioni della normativa in materia di protezione dei dati personali, tra cui carenze nell'informativa resa agli utenti, assenza di un'adeguata valutazione di impatto sulla protezione dei dati (DPIA), mancata adozione di misure di sicurezza adeguate e di idonee politiche di conservazione dei dati, nonché irregolarità nella designazione del responsabile del trattamento. Oltre alle sanzioni, l'Autorità ha ingiunto alle società di cessare i trattamenti oggetto di contestazione, ove non vi abbiano già provveduto, e di adeguarsi alle prescrizioni in materia di conservazione dei dati, dandone comunicazione al Garante. La replica della società non si è fatta attendere - «Poste Italiane accoglie con stupore il provvedimento con il quale il Garante Privacy ha comminato una sanzione per un presunto trattamento illecito dei dati personali degli utenti BancoPosta e PostePay. Provvedimento che, peraltro, oltre che nel merito, è viziato anche sotto il profilo procedimentale, essendo stato adottato in palese ritardo rispetto ai termini perentori previsti dalla legge per l'esercizio dei poteri del Garante», si legge in una nota diffusa dal gruppo dei recapiti. «A tal riguardo, si sottolinea che il 2 febbraio 2026 il Tar Lazio ha annullato il provvedimento con cui l'Antitrust aveva sanzionato Poste Italiane per una presunta pratica commerciale scorretta relativa al medesimo dispositivo antifrode oggetto delle odierne censure del Garante, riconoscendone la piena legittimità e l'assenza di qualsivoglia intento commerciale nelle condotte di Poste», si afferma nella nota diramata da Poste italiane. Poste Italiane «respinge ogni addebito e ribadisce la correttezza e la trasparenza del proprio operato. In particolare, come riconosciuto anche da Banca d'Italia, il Gruppo ha utilizzato legittimamente e in conformità con la normativa in materia di servizi di pagamento l'accesso ai dati tecnici dei dispositivi dei clienti, finalizzati esclusivamente all'attivazione di presidi antifrode e antimalaware, come richiesto dalla normativa europea (Direttiva PSD2), per una piena tutela della sicurezza degli utenti». Infine il gruppo dei recapiti annuncia che «presenterà ricorso per l'annullamento del provvedimento presso il Tribunale di Roma».
Fonte: Garante Privacy

Inchiesta "escort di lusso" a Milano: il Garante della privacy richiama i media

In riferimento alle notizie di stampa riguardanti l'inchiesta sulle "escort di lusso" a Milano in cui si riportano i nomi delle persone a vario titolo coinvolte, anche se non indagate, con un comunicato stampa il Garante per la protezione dei dati personali richiama i media e i siti web al più rigoroso rispetto della normativa privacy e delle Regole deontologiche, evitando di ledere la riservatezza e la dignità delle persone interessate.
Nel ribadire il legittimo esercizio del diritto-dovere del giornalista di informare su casi di interesse pubblico, l'Autorità "invita gli organi di stampa al rispetto del principio di essenzialità dell'informazione, in base al quale la diffusione di dati personali deve essere limitata a quanto strettamente indispensabile per la comprensione dei fatti di cronaca, evitando riferimenti eccedenti o non pertinenti".
Fonte: Garante Privacy

ROUTER DOMESTICI e **DATI INVISIBILI**, la **PRIVACY** si gioca anche sul terreno dei metadati e delle infrastrutture

> I **metadati** generati dal router **permettono di costruire un profilo attendibile** senza accedere direttamente a ciò che è stato scritto, detto o cercato e la privacy, in questo scenario, si sposta dal contenuto alla struttura dell'informazione

CONTINUA ON-LINE LA LETTURA

Nelle indagini sull'avvelenamento da ricina che ha colpito la comunità di Pietracatella, uno degli elementi più rilevanti è rappresentato dal recente sequestro dei router presenti nell'abitazione, per la ricostruzione del contesto informativo e relazionale entro cui si inserisce il grave fatto. Pur sembrando un semplice accessorio tecnico, il router è una possibile fonte autonoma di dati, capace di offrire una chiave di lettura alternativa e più ampia rispetto ai singoli dispositivi. Un'infrastruttura percepita come neutra può diventare fonte sistematica di trattamento di dati personali al di fuori di qualsiasi reale consapevolezza.

Il router oltre la connettività: una memoria digitale della casa - Il router costituisce un punto di concentrazione del traffico digitale domestico e, proprio per questo, una vera e propria memoria tecnica delle attività che si svolgono all'interno della rete. Pur non conservando necessariamente i contenuti delle comunicazioni, registra ciò che le rende intellegibili nel loro contesto: presenza dei dispositivi, tempi delle connessioni, relazioni tra nodi della rete. Anche se non racconta direttamente cosa accade, consente di ricostruirlo. Quali dati raccoglie davvero un router domestico - Un router domestico può conservare e rendere accessibili una serie articolata di informazioni tecniche. I dati raccolti riguardano i dispositivi collegati (identificati attraverso indirizzi MAC o nomi assegnati), gli orari di accesso e disconnessione, gli indirizzi IP locali attribuiti ai singoli device, le destinazioni raggiunte attraverso le richieste di rete e i log di sistema (che possono includere tentativi di accesso, errori di autenticazione, modifiche di configurazione, altre informazioni di contesto).

Sapere quando un dispositivo si è collegato, quanto a lungo è rimasto attivo, verso quali servizi ha indirizzato il traffico e in quale ordine temporale si sono susseguite le connessioni permette di delineare una traccia comportamentale estremamente significativa.

Dal dato tecnico al dato personale - Dati che nascono come tecnici diventano dati personali nel momento in cui consentono di identificare, anche indirettamente, una persona o di ricostruirne le abitudini. Il nome di un dispositivo, la ricorrenza degli accessi in determinate fasce orarie, la presenza costante di un determinato terminale all'interno della rete domestica sono elementi che, se correlati, restituiscono un'immagine dettagliata della vita quotidiana.

I metadati generati dal router permettono di costruire un profilo attendibile senza accedere direttamente a ciò che è stato scritto, detto o cercato e la privacy, in questo scenario, si sposta dal contenuto alla struttura dell'informazione. C'è poi il livello di opacità che circonda questi dispositivi. I router domestici non sono generalmente accompagnati da informative privacy realmente comprensibili o accessibili per gli utenti finali. La raccolta di metadati avviene nella sostanziale inconsapevolezza dell'interessato, che difficilmente è in grado di comprendere quali informazioni vengano trattate, per quali finalità e con quali possibili implicazioni. Il router come "scatola nera domestica" - In una vicenda come quella di Pietracatella, in cui è plausibile ipotizzare una fase preparatoria articolata, la possibilità di ricostruire le attività digitali attraverso i log di rete diventa particolarmente significativa. Anche in assenza di evidenze dirette sui dispositivi personali, la rete può restituire una narrazione indiretta, fondata su correlazioni temporali e relazionali.

Il router si configura come una sorta di "scatola nera domestica", capace di documentare la presenza dei dispositivi, la sequenza delle connessioni e le interazioni con l'esterno, configurando una forma di prova che si basa sulla struttura del comportamento digitale, come tale più resistente a tentativi di cancellazione o manipolazione.

.... continua a leggere online

Fonte: Articolo di Tania Orrù, Membro del Gruppo di Lavoro Federprivacy per la privacy nel marketing e nel commercio elettronico

nextbit
ICT & CONSULTING

Gestione dei dati • Sicurezza • Privacy/GDPR • Efficienza

visita il nostro sito
www.nextbitsrl.it

Nextbit per il Non Profit

Servizi e sistemi integrati per il Terzo Settore.

L'Attenzione all'evoluzione tecnologica, alle normative vigenti, ai benefici riservati al Non Profit ci consente di proporre soluzioni innovative, sicure, efficienti ed adeguate!

Alcuni argomenti che puoi affrontare insieme a noi:

software applicativo

- Gestione donatori e raccolta fondi
- Gestione associativa
- Gestione dei progetti
- Gestione contabile
- Controllo di gestione
- Rendicontazioni

comunicazione sociale

- Siti web & e-commerce
- Advertising per raccolta fondi
- Mail marketing
- Video emozionali
- Servizi grafici e fotografici

compliance & sicurezza

- Consulenza privacy
- Ottimizzazione dei processi
- Organizzazione documentale
- Sicurezza dei dati

nextbit ICT & CONSULTING
Nextbit Srl • Via I° Maggio, 4 - 06089 Torgiano (Perugia)
e-mail: info@nextbitsrl.it | **telefono:** 075 9975315 | **fax:** 075 395903 | P.IVA: 03097330546

TRACKING PIXEL NELLE E-MAIL: il banco di prova del consenso digitale nelle Linee guida del Garante

Con il provvedimento n. 284 del 17 aprile 2026 adottato ai sensi dell'art. 154-bis, comma 1, lett. a) del Codice e pubblicato nella Gazzetta Ufficiale n. 98 del 29 aprile 2026, il Garante per la protezione dei dati personali interviene per la prima volta in modo organico sull'uso dei pixel di tracciamento ("tracking pixel") nelle comunicazioni di posta elettronica. L'intervento colma un'evidente lacuna regolatoria: a fronte di una prassi divenuta pressoché universale – come accertato dall'Autorità nelle ispezioni conoscitive condotte nei mesi di ottobre 2025 e febbraio 2026 presso un provider e una piattaforma di marketing automation – mancava finora una disciplina dedicata, paragonabile a quella già introdotta per i cookie con le Linee guida del 10 giugno 2021 (provv. n. 231/2021, in G.U. n. 163 del 9 luglio 2021, doc. web n. 9677876). La cornice è ora delineata, e i soggetti tenuti dispongono di un termine di sei mesi dalla pubblicazione in Gazzetta Ufficiale, vale a dire fino al 29 ottobre 2026, per allineare sistemi, informative e flussi di consenso. I tracking pixel sono immagini di dimensioni minime – tipicamente trasparenti e di un solo pixel – non incorporate nel corpo dell'e-mail ma ospitate su server remoti. All'apertura del messaggio, un comando HTML innesca una richiesta automatica al server del mittente: l'immagine viene scaricata dal client di posta dell'utente e archiviata nella memoria del terminale. La stringa di richiesta tecnica che ne consegue veicola informazioni sull'avvenuta apertura, sull'indirizzo IP, sul dispositivo, sul tempo di consultazione e sul numero di aperture successive, oltre a parametri ulteriori (user ID, message ID, time stamp, token di sicurezza). Il Garante sottolinea, con considerazione di particolare rilievo nell'economia del provvedimento, che il profilo di maggiore criticità non risiede tanto nel contenuto delle inferenze ricavabili, quanto nel "carattere nascosto" del marcatore: la pervasività del pixel deriva, prima di ogni altra cosa, dalla mancata consapevolezza del destinatario, in violazione del principio di correttezza di cui all'art. 5, par. 1, lett. a), del Regolamento (UE) 2016/679. Il punto qualificante delle Linee guida è la qualificazione tecnico-giuridica delle operazioni effettuate per il tramite del pixel.

> ***Cosa sono i tracking pixel?***
> ***Sono immagini di dimensioni minime, tipicamente trasparenti e di un solo pixel, non incorporate nel corpo dell'e-mail ma ospitate su server remoti***

L'inserimento del marcatore nell'e-mail integra un'archiviazione di informazioni nel terminale dell'utente; la successiva lettura dei dati di ritorno costituisce accesso a informazioni archiviate. Entrambe le operazioni rientrano nella fattispecie dell'art. 122 del Codice (d.lgs. 196/2003), norma di recepimento della direttiva 2002/58/CE come modificata dalla direttiva 2009/136/CE. In coerenza con quanto già affermato dall'EDPB nelle Linee guida 2/2023 del 7 ottobre 2024 sull'ambito di applicazione tecnico dell'art. 5, par. 3, della direttiva e-Privacy, il Garante ribadisce che la disciplina e-Privacy, in quanto lex specialis, prevale sulle disposizioni del GDPR, ai sensi del considerando 173 e dell'art. 95 del Regolamento. Il GDPR resta tuttavia pienamente operativo come cornice generale, in particolare per i principi di correttezza e trasparenza, per i requisiti di validità del consenso (artt. 4, punto 11), e 7), per gli obblighi informativi (artt. 12 ss.) e per la privacy by design e by default (art. 25). La doppia chiave di lettura – e-Privacy/GDPR – è del resto coerente con il considerando 30 del Regolamento, espressamente richiamato dal Garante, che riconosce nel monitoraggio mediante identificativi online uno strumento idoneo, da solo o in combinazione con altri dati, alla profilazione e all'identificabilità dell'interessato.

Le Linee guida individuano una pluralità di figure che a vario titolo intervengono nella catena del trattamento: il mittente del messaggio, il fornitore di servizi di emailing in modalità SaaS, il fornitore di liste in noleggio, il fornitore della tecnologia di tracciamento, il content creator e infine il destinatario. La definizione caso per caso dei rispettivi ruoli – titolare, contitolare ex art. 26 GDPR, responsabile ex art. 28 GDPR – rappresenta un esercizio di accountability ai sensi dell'art. 5, par. 2 del Regolamento, e impone una rigorosa mappatura contrattuale. Si tratta di un punto sul quale i DPO dovranno esercitare particolare attenzione: la diffusione di catene complesse, in cui il committente affida a terzi sia la piattaforma di invio sia la tecnologia di tracciamento, rende cruciale evitare aree grigie nell'attribuzione delle responsabilità. Sul piano dell'informativa, il Garante – in continuità con l'approccio già seguito per i cookie – favorisce l'adozione di forme agevolate e multilivello. L'informazione potrà essere fornita in forma sintetica nel modulo di raccolta dell'indirizzo, con rinvio mediante link a contenuti più dettagliati anche all'interno della cookie policy esistente, e potrà avvalersi di canali multipli (pop-up, video, chatbot, assistenti virtuali). Resta fermo l'onere di responsabilizzazione del titolare, che dovrà valutare la concreta idoneità delle modalità prescelte sotto il profilo della completezza, della chiarezza espositiva e dell'efficacia. Per i trattamenti già in corso, l'informativa potrà essere veicolata con il primo invio utile o nel primo momento di discontinuità della relazione con l'interessato. Il comma 2-bis dell'art. 122 sancisce un divieto generalizzato di accesso al terminale dell'utente, salvo il ricorrere di una delle ipotesi tassative previste dal comma 1: il consenso preventivo dell'utente – che deve essere libero, specifico, informato e inequivocabile, ai sensi dell'art. 4, punto 11) GDPR; la necessità del trattamento ai fini della trasmissione della comunicazione elettronica; la stretta necessità per la fornitura di un servizio della società dell'informazione esplicitamente richiesto dall'utente. È su questa griglia regola-deroga che si articola l'intera architettura del provvedimento. Allo stato attuale delle conoscenze – e con espressa riserva di aggiornamento – il Garante individua tre ipotesi concrete in cui i titolari possono legittimamente impiegare tracking pixel senza acquisire il consenso. La prima è la misurazione statistica aggregata orientata al miglioramento della deliverability e al contrasto dello spam, a condizione che il pixel sia univoco per la campagna (uguale per tutti i destinatari) e che indirizzo IP e altri dati tecnici siano anonimizzati conformemente al Parere WP29 n. 05/2014 sulle tecniche di anonimizzazione. La seconda è l'impiego del pixel come misura di sicurezza nei processi di autenticazione, attivazione di account, gestione di richieste di modifica password o esercizio dei diritti dell'interessato (compresa la portabilità): qui la verifica dell'effettiva apertura sul terminale legittimo dell'utente esplica una funzione di sicurezza accessoria al servizio richiesto. La terza, di particolare rilievo per i soggetti pubblici e per i settori regolati (banche e intermediari in primis), riguarda i messaggi istituzionali o di servizio caratterizzati da un obbligo giuridico di inoltro – modifiche contrattuali, comunicazioni di sicurezza, notifiche di incidenti, allerte antifrode, scadenze contributive – per i quali il riscontro dell'effettiva presa di conoscenza concorre alla tutela dell'interessato medesimo. Quando non ricorra una delle ipotesi di deroga, il consenso è dovuto. Il Garante affronta tuttavia, con apprezzabile pragmatismo, la questione della duplicazione fra consenso al messaggio promozionale e consenso al pixel. La stretta correlazione finalistica e l'esigenza di evitare meccanismi di pressione sull'interessato consentono, in linea di principio, di ricomporre i due consensi in un'unica manifestazione di volontà, purché formulata in modo neutro e privo di forzature. Si tratta di una soluzione sensibile alla logica di semplificazione e coerente con la giurisprudenza dell'EDPB sul principio del consenso libero e specifico: l'unicità del consenso non deve diventare scappatoia per pacchetti opachi, ma punto di equilibrio tra esigenze di chiarezza e tutela effettiva. Se l'ammissibilità del consenso unitario costituisce un'apertura, il Garante chiede in compenso che la revoca sia granulare. L'interessato deve poter scegliere, in ogni momento, fra tre opzioni: continuare a ricevere comunicazioni con tracciamento, continuare a riceverle senza tracciamento, ovvero cessare del tutto la ricezione. A questo fine, ogni e-mail deve recare – tipicamente nel footer – un'icona standardizzata o un link che conduca a un'area dedicata all'esercizio dei diritti. Il rifiuto del solo tracciamento non può comportare alcuna limitazione del servizio. È quanto emerge anche dal confronto, ormai esplicito nel dibattito europeo, con la Raccomandazione della CNIL francese del 12 marzo 2026: entrambe le autorità impongono un meccanismo di opt-out raggiungibile dal footer, ma il Garante italiano si spinge oltre, costruendo la granularità come autonomo diritto dell'interessato, distinto dal diritto di disiscrizione. .... *continua a leggere online*

Michele Iaselli
Coordinatore del Comitato Scientifico di Federprivacy

CONTINUA ON-LINE
LA LETTURA

La Privacy oltre la teoria: consulenza concreta per il tuo business

Nimaja Consulting e Privacy Solutions S.r.l.: l'unione di due eccellenze al servizio della conformità aziendale

Expertise in Privacy e Compliance Assicurativa: Specializzati nella gestione dei flussi per intermediari assicurativi. Un metodo rigoroso e collaudato, applicabile con successo a ogni business.

Impianti Privacy a 360°: Modelli di gestione dati personalizzati, studiati per adattarsi con efficacia sia alla realtà della micro-azienda che alla complessità delle grandi organizzazioni.

Whistleblowing: Implementazione della nostra piattaforma proprietaria sicura e conforme, con gestione professionale affidata a un WB Manager dedicato.

Consulenza, non Burocrazia: Traduciamo il GDPR in processi snelli, pensati per chi deve lavorare, non solo compilare moduli.

NIMAJA CONSULTING

Privacy Solutions S.r.l.
Soluzioni per i tuoi dati

Web: www.nimajaconsulting.it - Email: info@nimajaconsulting.it - Tel: +39 011 19878291

Sanzionata per **VIOLAZIONE** della **PRIVACY** l'**AZIENDA** che **IMPONE** al **DIPENDENTE** di utilizzare lo **SMARTPHONE PERSONALE** come **STRUMENTO** di **LAVORO**

Nella società digitale, in cui il lavoro passa sempre più attraverso app, dispositivi mobili e piattaforme online, **la protezione dei dati personali diventa** quindi un terreno cruciale di **equilibrio tra innovazione e diritti**

LEGGI ON-LINE

C'è una linea sottile che separa l'organizzazione del lavoro dal controllo pervasivo della vita privata. Sempre più spesso il confine passa per lo smartphone che abbiamo in tasca: non solo uno strumento di comunicazione, ma un archivio intimo di abitudini, spostamenti e relazioni.

Quando entra nel perimetro aziendale, il rischio è che diventi una finestra costantemente aperta sulla sfera personale dei dipendenti, se non una vera e propria spia.

Ne è una dimostrazione la recente sanzione di 200.000 euro inflitta dall'Agencia Española de Protección de Datos (AEPD) alla Ares Capital, società di noleggio veicoli con conducente (NCC), per aver imposto ai lavoratori l'uso del proprio telefono personale, obbligandoli a installarvi applicazioni di monitoraggio.

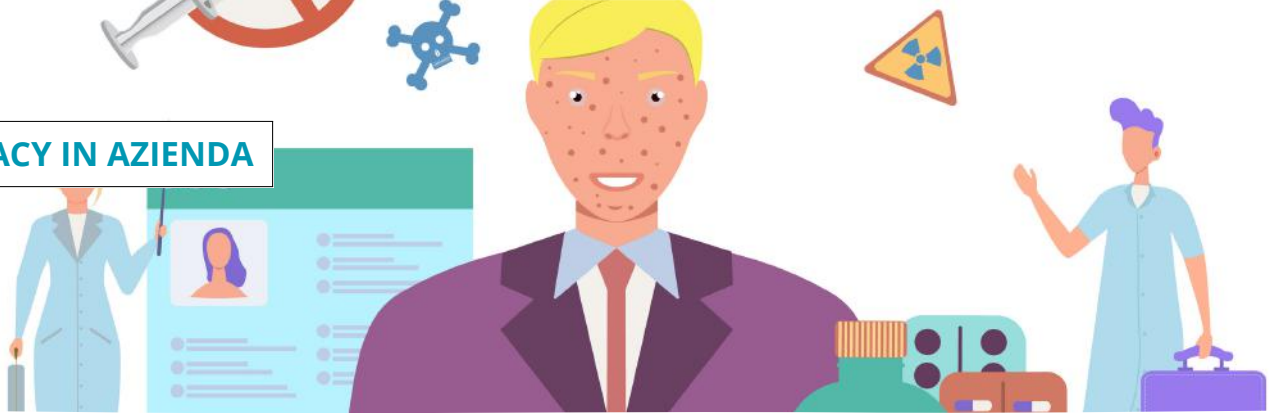
Dietro quella che l'azienda presentava come una semplice esigenza organizzativa – gestione dei turni, controllo e sicurezza – si celava un sistema di raccolta dati molto più ampio. Le app erano infatti in grado di tracciare la geolocalizzazione in modo continuo, registrare comunicazioni, accedere a immagini e raccogliere informazioni sullo stato fisico degli utenti.

Un livello di intrusione che travalicava i limiti del lecito. Il punto centrale della decisione riguarda il principio di minimizzazione dei dati (art. 5 del GDPR), secondo cui un datore di lavoro può trattare solo le informazioni strettamente necessarie per la finalità dichiarata.

In questo caso, la raccolta risultava sproporzionata. Ma è soprattutto una questione di equilibrio tra potere datoriale e diritti fondamentali. L'utilizzo del dispositivo personale per finalità lavorative introduce un cortocircuito: ciò che è privato diventa accessibile all'organizzazione.

E anche quando sussiste una base giuridica, come il consenso, resta il problema della libertà del lavoratore. Può davvero dirsi libero di rifiutare, quando da quella scelta dipende la possibilità stessa di lavorare? Nel caso esaminato, la società sosteneva di offrire in alternativa dispositivi aziendali, ma la loro disponibilità limitata rendeva la scelta del telefono privato di fatto obbligata. Un dettaglio cruciale per il Garante spagnolo: in contesti di asimmetria contrattuale, il consenso rischia di essere solo apparente, mentre l'art. 4 del GDPR rimarca che esso deve essere una "manifestazione di volontà libera, specifica, informata e inequivocabile". La vicenda si inserisce in un contesto in cui le tecnologie consentono forme di controllo capillari. Senza limiti adeguati, queste pratiche si trasformano in una sorveglianza continua, incompatibile con la dignità della persona. Negli ultimi anni, diverse decisioni delle autorità europee hanno ribadito che il datore di lavoro non può scaricare sui dipendenti i costi – economici e di privacy – degli strumenti di lavoro, né usare tecnologie invasive senza una rigorosa valutazione di proporzionalità. Quando un'azienda richiede l'uso del dispositivo privato, entra nel modello BYOD ("Bring Your Own Device"). Questo approccio comporta criticità che impongono il rispetto sia dell'art. 4 dello Statuto dei lavoratori sia del GDPR. Sul piano della protezione dei dati, la commistione espone a rischi di data breach, installazione di app invasive, controlli indiretti, accesso alla rubrica personale e difficoltà nel garantire il diritto alla disconnessione. Nella società digitale la protezione dei dati personali diventa un terreno cruciale di equilibrio. Per le imprese, la sfida non è solo evitare le sanzioni, ma ripensare i modelli organizzativi in chiave sostenibile e rispettosa dei lavoratori.

Fonte: Nòva Il Sole 24 Ore – Articolo di Nicola Bernardi, Presidente di Federprivacy



SANZIONI per VIOLAZIONi della PRIVACY nella SANITÀ, quando è il dirigente a dover pagare di tasca propria

> Nelle **organizzazioni pubbliche** contemporanee il **rischio non è** tanto l'**assenza di modelli privacy**, quanto la costruzione di apparati formalmente impeccabili ma sostanzialmente incapaci di incidere davvero sulla gestione tecnologica

LEGGI ON-LINE

Alla fine il dirigente finisce nell'angolo e deve pagare. Il dossier sanitario poco robusto presenta il conto, ma questa volta a pagare non è il DPO. La Corte dei conti di Bolzano, con la sentenza n. 7/2026, lancia infatti un messaggio destinato a fare rumore nelle pubbliche amministrazioni: la privacy non si salva con cabine di regia, regolamenti patinati e riunioni interminabili se poi nessuno mette mano ai sistemi informatici. La vicenda nasce dalla sanzione da 75 mila euro inflitta dal Garante privacy all'Azienda sanitaria dell'Alto Adige per accessi abusivi al dossier sanitario elettronico. Medici e operatori sanitari riuscivano a consultare dati di pazienti estranei ai rispettivi percorsi di cura grazie a un sistema basato su autodichiarazioni e privo di adeguati controlli automatici sugli accessi anomali. Una situazione che era già stata attenzionata dall'Autorità anni prima. Qui emerge il vero nodo della sentenza. Il problema non era l'assenza di strutture privacy, ma il fatto che queste sembravano vivere in un universo parallelo rispetto alla gestione tecnica del sistema informatico. La Corte ricostruisce un quadro emblematico: report, consulenze, regolamenti, mail e persino la previsione teorica di alert automatici. Tutto perfetto sulla carta, mentre gli accessi abusivi continuavano. I giudici contabili prendono così le distanze dalla diffusa tendenza burocratica a trasformare il GDPR in un gigantesco esercizio documentale. La sentenza chiarisce che l'accountability non coincide con la produzione seriale di atti formali, ma con la concreta capacità dell'ente di impedire trattamenti illeciti. In questo quadro la posizione del DPO e della referente privacy viene ridimensionata sotto il profilo della responsabilità erariale.

La Corte evidenzia come tali soggetti avessero ripetutamente segnalato le criticità e richiesto interventi correttivi alla struttura informatica, pur mancando di un effettivo potere gerarchico o gestionale idoneo a imporre le modifiche tecniche necessarie. Un passaggio cruciale, che contrasta la pericolosa tendenza a trasformare il DPO nel parafulmine universale dell'ente. La sentenza rimette ordine nei ruoli: il DPO consiglia, segnala, monitora, ma se chi gestisce l'organizzazione ignora le segnalazioni, la responsabilità non può essere scaricata a valle. Il bersaglio principale della Corte diventa quindi il direttore della ripartizione informatica, ritenuto il soggetto concretamente investito dei poteri di coordinamento e impulso necessari ad adeguare il sistema. La motivazione è severissima: il dirigente non può difendersi sostenendo di non avere competenze operative dirette o di non essere amministratore di sistema. Un dirigente resta responsabile se omette di impartire direttive o pretendere l'attuazione delle misure necessarie. Non basta inoltrare email o convocare riunioni; occorre assumersi la responsabilità di chiudere le falle tecnologiche. La Corte conclude che gli accessi abusivi sono stati causati dall'omessa adozione delle misure richieste per anni dalla cabina di regia privacy. Viene invece assolto il direttore generale, poiché la struttura privacy appariva formalmente idonea e non emergevano elementi che dimostrassero una sua piena consapevolezza delle criticità tecniche. E qui si palesa il grande tema della sentenza: il rischio reale non è l'assenza di modelli privacy, quanto la costruzione di apparati impeccabili ma incapaci di incidere sulla gestione tecnologica.

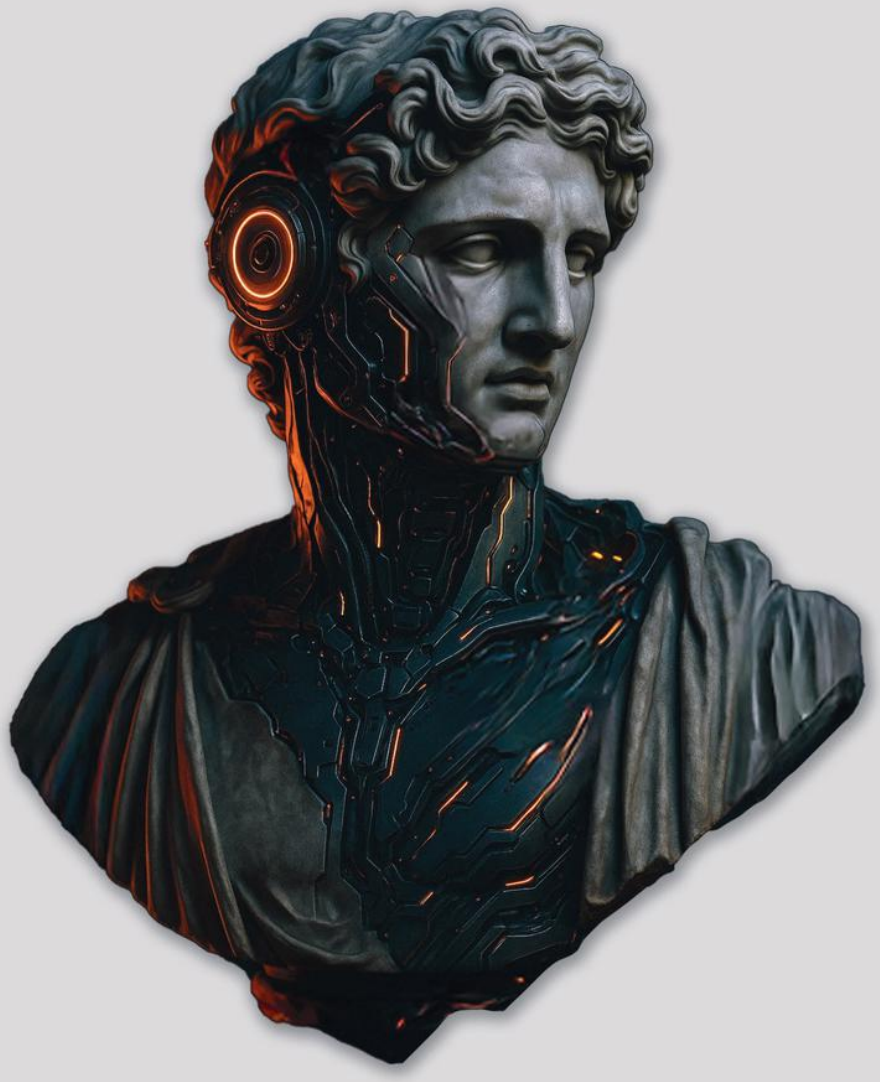
Fonte: Articolo di Stefano Manzelli, Direttore di sicurezzaurbanaintegrata.it

ICTLC

ICT LEGAL CONSULTING

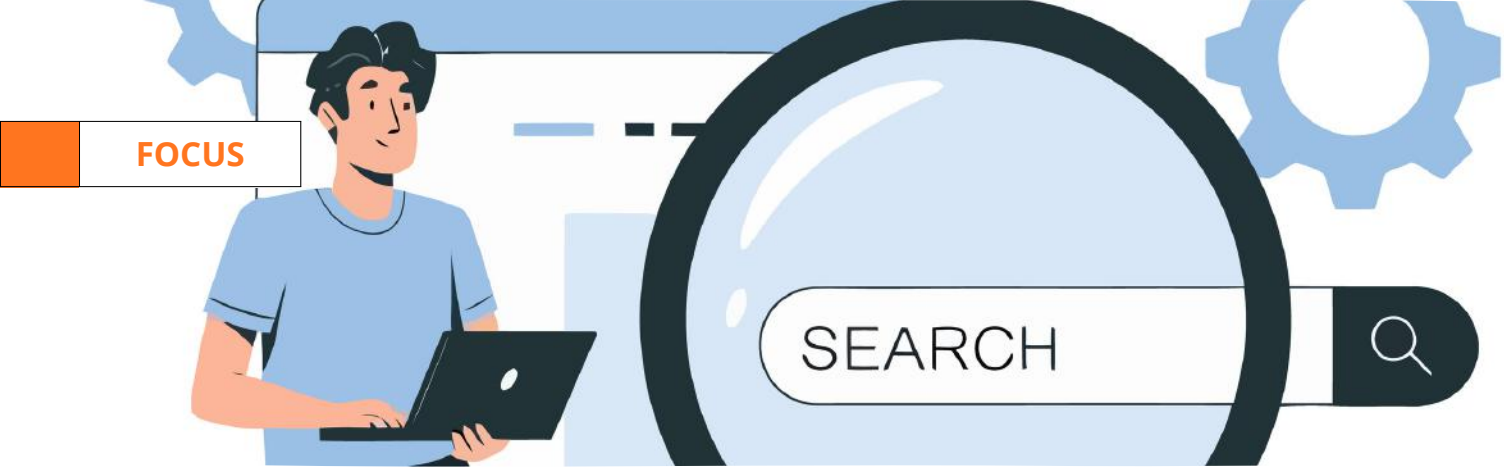
ICT CYBER CONSULTING

Consulenza strategica, integrata e globale
in materia di protezione e valorizzazione dei
dati, cybersecurity e intelligenza artificiale.



L'eccellenza non è un atto,
ma un'abitudine.

www.ictlc.com



DANNO da **TARDIVA DEINDICIZZAZIONE** sui **MOTORI DI RICERCA**, prova del pregiudizio anche mediante presunzioni semplici

La **Cassazione** chiarisce che il danno da ritardata deindicizzazione è risarcibile: **il pregiudizio alla reputazione può essere dimostrato anche tramite presunzioni semplici**, senza automatismi ma valutando la gravità della lesione

Con l'ordinanza 6433 del 18 marzo 2026, la Corte di Cassazione ha cassato la sentenza nella quale il Tribunale di Roma negava a un utente il risarcimento del danno da ritardata deindicizzazione di articoli di stampa che lo riguardavano. La vicenda origina dalla richiesta di deindicizzazione avanzata al motore di ricerca Google da un soggetto coinvolto in un procedimento penale conclusosi con declaratoria di estinzione per prescrizione. I gestori dei motori di ricerca, infatti, sono tenuti a garantire un tempestivo riscontro alle istanze di deindicizzazione da parte degli utenti che invochino motivatamente il proprio diritto all'oblio. Come è noto, l'attuazione del diritto all'oblio non implica la cancellazione della notizia dalla fonte originaria, ma la sua rimozione dai risultati di ricerca associati al nome dell'interessato, al fine di evitare una indebita e permanente esposizione mediatica. Nonostante la presentazione di idonea domanda di deindicizzazione da parte dell'utente, il motore di ricerca aveva lasciato i contenuti accessibili per un lungo periodo, determinando, secondo l'utente, la lesione alla propria reputazione e un illecito trattamento dei propri dati personali. Il Tribunale di Roma, pur riconoscendo la violazione del diritto all'oblio, aveva escluso il risarcimento del danno non patrimoniale per ritenuto difetto di prova del danno. Per contro, secondo i giudici di legittimità, l'affermazione circa la mancanza di prova del pregiudizio doveva ritenersi di mero stile, e risulta incompatibile con il previo accertamento dell'illecito operato dal Tribunale.

In particolare, nella pronuncia in commento si evidenzia come il giudice di merito abbia omesso di valutare elementi fattuali rilevanti, quali la diffusione delle informazioni, la loro non attualità e l'impatto sulla reputazione del soggetto interessato. La Cassazione ribadisce quindi che in materia di trattamento illecito dei dati personali e lesione della reputazione, il pregiudizio può essere provato dal danneggiato anche mediante presunzioni, ove siano allegate circostanze oggettive, tra cui l'ampia visibilità dei contenuti rimasti online e la loro idoneità a incidere negativamente sui diritti della personalità dell'individuo.

Sotto il profilo probatorio, la prova del danno non patrimoniale è di regola fornita mediante documentazione medica attestante una lesione all'integrità psicofisica oppure situazioni di ansia e stress tali da richiedere, ad esempio, la prescrizione di specifici farmaci. In ogni caso, come accennato, il giudice può ritenere provato il danno anche in assenza di documentazione sanitaria, facendo ricorso a presunzioni semplici, qualora le regole di esperienza consentano di ritenere verosimile la sofferenza patita dal soggetto leso in conseguenza dell'illecito trattamento dei dati personali (ad esempio nel caso di illegittima diffusione di dati relativi alla grave patologia di una persona).

Giova evidenziare che con la pronuncia in esame la Corte non ha sancito un automatismo nella risarcibilità del danno da illecito trattamento dei dati personali.

Come sancito da consolidata giurisprudenza, infatti, il diritto al risarcimento del danno non si sottrae alla previa verifica, da parte del giudice, della serietà del danno e della gravità della lesione.

APPROFONDIMENTO GRATUITO PER GLI UTENTI DEL SITO FEDERPRIVACY

Fonte: Il Sole 24 Ore – Articolo di Alessandro Candini, Studio Legale Finocchiaro

Innovazione tecnologica e tocco umano: la regola dell'equilibrio

Proteggi i tuoi dati, costruisci fiducia, promuovi sostenibilità

In un contesto in cui l'incertezza su come vengono raccolti e usati i nostri dati è sempre più diffusa, diventa fondamentale costruire fiducia. E questa fiducia non si può imporre: si conquista attraverso la trasparenza, la verifica indipendente e un'educazione digitale consapevole tra cittadini, istituzioni e soprattutto le imprese. Affidati all'esperienza di TÜV Italia per integrare la privacy e la cybersecurity nelle tue strategie di impresa, attraverso i servizi di:

- valutazione
- audit e certificazioni di sistema
- formazione
- certificazione delle persone
- servizi per la sostenibilità

Contattaci per scoprire come possiamo supportarti.

TÜV Italia srl
Viale Fulvio Testi 280/6 - 20126 Milano
tuv.ms@tuvsud.com - tuv.formazione@tuvsud.com
www.tuvsud.com/it

Quando **PROCEDURE** e **LINEE GUIDA** sono **DISALLINEATE** dalle **PRASSI REALI** **AUMENTANO** i **RISCHI** organizzativi e privacy

> Per l'**EDPB**, la soluzione più conforme al GDPR è chiara: **la piattaforma di shopping online deve permettere all'utente di acquistare come ospite**

La sentenza n. 167 del 13 aprile 2026 del Tribunale di Udine – Sezione Lavoro, è intervenuta su una vicenda disciplinare relativa all'utilizzo di WhatsApp da parte di una lavoratrice per comunicare il protrarsi della propria assenza. La dipendente aveva inviato messaggi vocali e documentazione a un referente aziendale che aveva ricevuto le comunicazioni, interagito con lei e organizzato le sostituzioni operative. Solo successivamente l'azienda aveva contestato l'utilizzo del canale, richiamando procedure interne che prevedevano modalità differenti. Il Tribunale ha tuttavia osservato come tali procedure, pur formalmente esistenti, non risultassero concretamente presidiate nella fisiologia organizzativa dell'ente, essendo risultate, nella prassi organizzativa, tollerate modalità comunicative differenti rispetto a quelle formalmente previste, senza che tali deviazioni fossero concretamente contrastate. La decisione assume quindi rilievo non tanto per il mero utilizzo di WhatsApp, quanto perché consente di evidenziare un fenomeno sempre più frequente nelle organizzazioni contemporanee: il progressivo disallineamento tra procedure ufficiali, governance dichiarata e prassi operative reali. Ciò può determinare una significativa vulnerabilità organizzativa quando l'ente perde la capacità di rappresentare, presidiare e controllare le modalità effettive attraverso cui dati, comunicazioni e decisioni vengono concretamente gestiti È in questa prospettiva, e non con riferimento diretto alla specifica vicenda giudiziaria, che assume rilievo anche per la protezione dei dati personali post-2018 la questione dei flussi informativi che iniziano a svilupparsi attraverso ecosistemi relazionali paralleli, tollerati ma non realmente governati. Il GDPR ha progressivamente trasformato la protezione dei dati personali in una disciplina di governo dei processi informativi, come emerge dalla logica combinata degli artt. 5, 24, 25 e 32 del Regolamento UE.

Accountability, privacy by design e misure organizzative adeguate non richiedono soltanto procedure formalmente corrette, ma assetti concretamente capaci di governare i flussi informativi reali.

Il tema non riguarda soltanto informative, registri o adempimenti documentali. Riguarda, più profondamente, la capacità dell'organizzazione di mantenere conoscibilità, tracciabilità e governabilità dei trattamenti effettivamente svolti.

Il problema organizzativo emerge soprattutto quando la deviazione dalla procedura non è episodica, ma diventa prassi organizzativa tacitamente accettata. In tali situazioni, il rischio non consiste soltanto nella violazione della singola regola, ma nella progressiva perdita di corrispondenza tra modello organizzativo formale e funzionamento reale dell'ente.

In questo scenario si inserisce anche il fenomeno dello "shadow IT".

L'utilizzo di strumenti informali o sviluppati autonomamente dagli utenti aziendali, così come di canali comunicativi alternativi, non nasce spesso da una volontà elusiva, ma dalla necessità di mantenere rapidità decisionale e continuità operativa all'interno di processi che le architetture ufficiali non riescono più a sostenere efficacemente.

Per questa ragione, le funzioni di secondo livello — compliance, privacy office, Operational Risk Management e cybersecurity governance — non possono limitarsi a una verifica meramente documentale della conformità.

In tale contesto, con riguardo ai dati personali, il Responsabile della protezione dei dati, nell'ambito delle proprie funzioni di sorveglianza e consulenza previste dall'art. 39 GDPR, è una delle poche figure chiamate a osservare in maniera trasversale i trattamenti, i flussi informativi e la coerenza tra processi dichiarati e processi concretamente esercitati. *.... continua a leggere online*

CONTINUA ON-LINE LA LETTURA

Fonte: Articolo di Pasquale Mancino, Componente del Gruppo di Lavoro per la privacy nella Pubblica Amministrazione

datapro

#YourDataProtectionOfficer

ISO 9001
LL-C (Certification)

ISO 27001
LL-C (Certification)

Specialisti in Data Protection

Team di consulenti certificati con competenze multidisciplinari in ambito normativo, tecnologico e di organizzazione aziendale

Realizziamo ed implementiamo le strategie di Data Protection per il Business, attraverso:

- **COMPLIANCE NORMATIVA**
Regolamento Europeo - GDPR UE 2016/679
Futuro Regolamento ePrivacy

- **VALUTAZIONI D'IMPATTO**
con l'analisi approfondita del sistema informativo siamo in grado di produrre una valutazione del rischio esaustiva e suggerire le necessarie migliorie

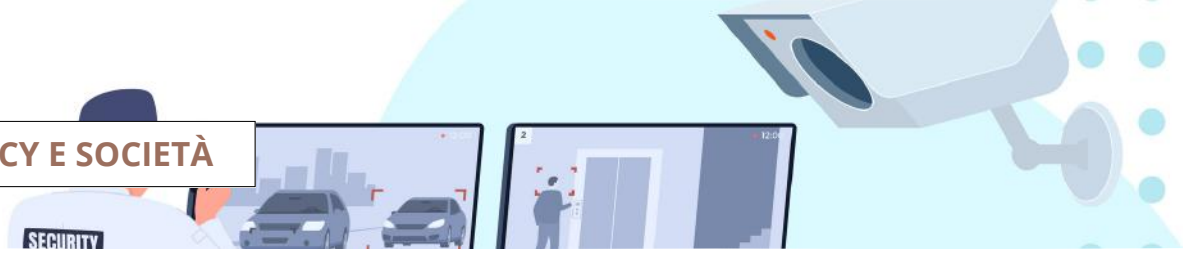
- **CYBERSECURITY E CONTROLLI**
Implementiamo auditor di sistema per monitorare il livello di sicurezza delle informazioni aziendali progettiamo i controlli che, nel rispetto della Privacy, permettano di prevenire azioni dannose

- **CERTIFICAZIONI**
accompagniamo le organizzazioni verso la massima protezione dei dati portandole a raggiungere la Certificazione ISO/IEC 27001:2017

- **VERIFICHE PERIODICHE**
garantiamo nel tempo i livelli di compliance raggiunti e suggeriamo gli opportuni miglioramenti

www.dataprogdpr.com • consulenza@datapro.srl

MILANO - PIACENZA - PARMA - REGGIO EMILIA - MODENA - BOLOGNA
FORLI' CESENA - RIMINI - RAVENNA - VERONA - PISA



VIOLA il **GDPR** l'**IMPIANTO** di **VIDEOSORVEGLIANZA** dotato di un **SOLO CARTELLO** per segnalare più telecamere installate in vari ambienti

Con il **provvedimento n. 167/2026** il Garante per la protezione dei dati personali ha sanzionato una società di ristorazione per una gestione non conforme delle telecamere installate nei propri locali.

Viola la privacy dei lavoratori l'impianto di videosorveglianza segnalato da un solo cartello informativo per più ambienti, con accesso alle immagini senza bisogno di credenziali di accesso, e soprattutto con l'autorizzazione dell'Ispettorato del lavoro ottenuta solo successivamente alla messa in funzione. A evidenziarlo è il provvedimento n. 167 del 12 marzo 2026 adottato dal Garante, che ha sanzionato una società di ristorazione per una gestione non conforme delle telecamere installate nei propri locali. Il caso prende avvio da un accertamento della Guardia di Finanza che, nel corso di un'ispezione, aveva rilevato la presenza di telecamere attive all'interno e all'esterno dell'esercizio commerciale, con lavoratori presenti nelle aree riprese.

Fin da subito, tuttavia, sono emerse criticità rilevanti: un solo cartello informativo per più ambienti, assenza di credenziali di accesso al sistema e, soprattutto, mancanza dell'autorizzazione dell'Ispettorato del lavoro al momento dell'installazione, intervenuta solo successivamente. Il provvedimento si colloca nel solco applicativo del GDPR e del Codice Privacy, richiamando in particolare i principi generali del Regolamento UE 2016/679, tra cui quello di trasparenza e quello dell'art. 13 riguardante le informazioni da rendere agli interessati. Nel caso esaminato, la presenza di un unico cartello, peraltro non collocato in modo da coprire tutte le aree sorvegliate, è stata ritenuta insufficiente a garantire una informativa effettiva. Non meno rilevante è il profilo della liceità del trattamento, analizzato alla luce dell'art. 88 del GDPR in materia di rapporti di lavoro e dell'art. 114 del Codice, che rinvia alla disciplina dello Statuto dei lavoratori. Come noto, l'art. 4 della Legge 300/1970 consente infatti l'uso di impianti audiovisivi solo previa stipula di un accordo sindacale o autorizzazione dell'Ispettorato del lavoro, qualora possa derivarne un controllo a distanza dei lavoratori. Nel caso di specie, l'impianto risultava già operativo prima del rilascio dell'autorizzazione, determinando una violazione del principio di liceità del trattamento.

Il Garante ribadisce così un orientamento consolidato: la procedura autorizzativa non rappresenta un mero adempimento formale che può essere espletato anche successivamente, ma una garanzia sostanziale posta a tutela della dignità dei lavoratori e dell'equilibrio tra potere datoriale e diritti fondamentali. La sua omissione incide direttamente sulla legittimità del trattamento dei dati personali. Ulteriore profilo critico riguarda la sicurezza dei dati. L'assenza di credenziali di accesso al sistema di videosorveglianza è stata ritenuta in contrasto con gli artt. 5, par. 1, lett. f) e 32 del GDPR, che impongono l'adozione di misure tecniche e organizzative adeguate. Senza un sistema di autenticazione, infatti, non è possibile tracciare gli accessi né limitare la visione delle immagini ai soli soggetti autorizzati, con evidenti rischi per la riservatezza degli interessati. Alla luce di tali violazioni, l'Autorità ha dichiarato l'illiceità del trattamento e irrogato una sanzione amministrativa pari a 2.000 euro, tenendo conto della natura colposa della condotta e dell'assenza di precedenti specifici. Nel provvedimento il Garante ha messo in evidenza come l'obbligo di trasparenza necessiti della predisposizione e messa in opera di idonei cartelli di "informativa minima", affinché gli interessati siano resi «consapevoli del fatto che è in funzione un sistema di videosorveglianza» prima di entrare nel perimetro di ripresa delle telecamere. Le informazioni più importanti devono essere indicate sul segnale di avvertimento cioè mediante cartelli visibili a tutti, collocati ad altezza delle persone e riguardano le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato. Come indicato nelle Linee Guida 3/2019 del EDPB, gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi. Questi ultimi, devono essere facilmente accessibili per l'interessato, ad esempio attraverso una pagina informativa completa messa a disposizione in uno luogo centrale o affissi in un luogo di facile accesso, o, infine, contenuti e riscontrabili in un codice QR o in un indirizzo web.

LEGGI ON-LINE

Fonte: Federprivacy

SCAN ME

www.essetiweb.it - www.mygdpr.online

SECURITY SERVICES

SICUREZZA E PROTEZIONE DEI TUOI DATI

ESSETI progetta e costruisce l'infrastruttura della tua azienda con tecnologie aderenti agli standard di sicurezza NIST Cybersecurity Framework
Per garantire la continuità della tua organizzazione abbiamo consolidato Partnership con i più importanti produttori specializzati per utilizzare tecnologie che assicurano un servizio di alta qualità.

CYBERSECURITY E THREAT INTELLIGENCE

La Soluzione di Cyber Security pensata per analizzare e prevenire potenziali minacce alla sicurezza delle informazioni all'interno ed all'esterno di un'organizzazione. Un servizio cloud "as a service" che permette di disporre di una piattaforma di Cyber Threat Intelligence in grado di controllare ed analizzare il livello di sicurezza di infrastrutture ICT, dati, processi informativi, identificare minacce in ambiente OSINT e Dark Web (ad es. data breach), cyber reputation, social engineering e criticità in ambienti fisici.

PROMO
CANONE SERVIZIO SAAS
PRIMO MESE GRATIS

CARATTERISTICHE DEL SERVIZIO

- MONITORAGGIO CONTINUO
- HOST / NETWORK / APPLICATION VULNERABILITY ASSESSMENT
- PENETRATION TEST AUTOMATIZZATO
- CYBER FEED E CYBER REPUTATION
- CYBER THREAT INTELLIGENCE
- ASSET MANAGEMENT
- REPORT, GOVERNANCE E COMPLIANCE
- DASHBOARD E CENTRO NOTIFICHE

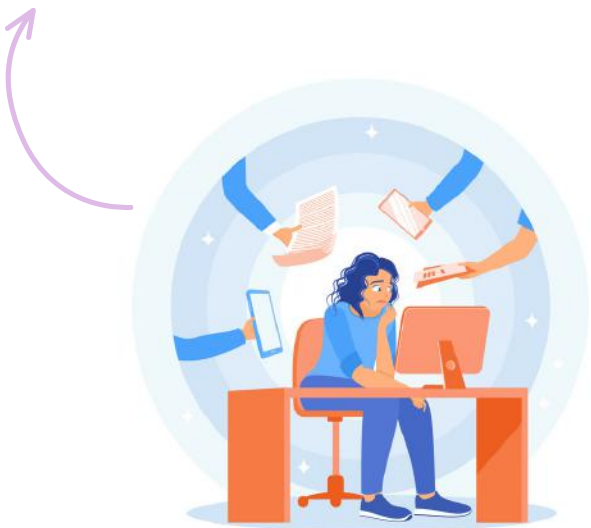
promozione primo mese servizio SaaS gratis valida fino al 31/07/2024

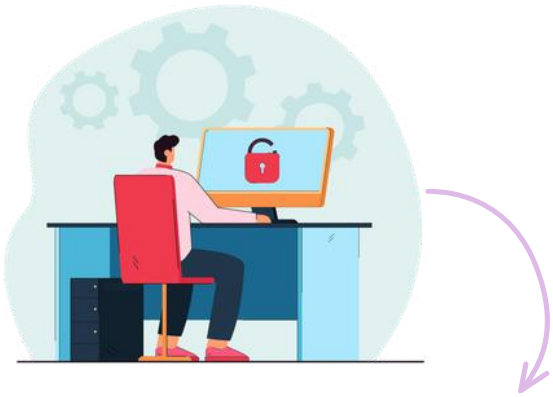
CONTATTACI
0577 931930
info@essetiweb.it

Esseti | Digital Transformation per le PMI | Consulenza e Servizi IT

SOTTO LA LENTE DEL GARANTE PRIVACY UNA START-UP CHE HA SVILUPPATO UN PLUG-IN IN GRADO DI RILEVARE LINGUAGGIO, EMOZIONI E LIVELLO DI STRESS DEI DIPENDENTI

Il Garante per la protezione dei dati personali ha inviato un avvertimento a una start-up italiana che ha sviluppato un componente aggiuntivo (plug-in) per le piattaforme di messaggistica aziendale Slack e Teams, finalizzato a rilevare, tramite intelligenza artificiale e analisi semantica delle chat, il livello di stress psicologico dei lavoratori che decidano volontariamente di utilizzarlo per ricevere suggerimenti personalizzati. Le verifiche dell'Autorità, avviate a seguito di notizie di stampa, hanno evidenziato che la start-up tratta i dati degli utenti del servizio in qualità di titolare del trattamento. Il datore di lavoro che acquista il servizio, invece, non può accedere né ai contenuti delle comunicazioni analizzate né ai risultati individuali elaborati dal sistema.
Considerata tuttavia la particolare delicatezza dei dati trattati, nonché la possibilità di fornire ai datori di lavoro report aggregati sul livello di stress dei dipendenti, il Garante ha invitato la società ad adottare, sin dalla progettazione del servizio, misure adeguate a prevenire ogni rischio di accesso, anche indiretto, a informazioni relative alla sfera emotiva dei lavoratori. Si tratta, infatti, di informazioni che il datore di lavoro non può legittimamente acquisire o trattare, in base alla normativa privacy, allo Statuto dei lavoratori e al Regolamento europeo sull'intelligenza artificiale, che vieta l'uso di sistemi di IA destinati a dedurre o analizzare le emozioni delle persone nei contesti lavorativi. Il Garante ha infine richiamato i rischi legati all'impiego di tecnologie basate su modelli linguistici e analisi semantica, che possono produrre risultati non sempre trasparenti, spiegabili o verificabili, con possibili effetti discriminatori o lesivi dei diritti dei lavoratori.
F*onte: Garante Privacy*





DAI COMMERCIALISTI IL DOCUMENTO "CYBERSECURITY E MODELLO 231: INTEGRAZIONE DEI RISCHI INFORMATICI NELLA GOVERNANCE D'IMPRESA"

Il Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili (CNDCEC) ha pubblicato il documento "Cybersecurity e Modello 231: integrazione dei rischi informatici nella governance d'impresa", elaborato dalla Commissione di studio "Compliance e modelli organizzativi d.lgs. 231" nell'ambito dell'area di delega "Compliance e modelli organizzativi delle imprese", cui sono delegati i consiglieri nazionali Fabrizio Escheri ed Eliana Quintili. "Le minacce informatiche rappresentano oggi un fattore di rischio strategico per le imprese e impongono un approccio sempre più integrato tra sistemi di controllo interno, governance e compliance –, afferma il presidente del Consiglio Nazionale dei Commercialisti, Elbano de Nuccio –. Con questo documento intendiamo offrire ai professionisti uno strumento utile ad accompagnare le imprese nella gestione del rischio cyber e nell'adeguamento dei modelli organizzativi ai più recenti sviluppi normativi e tecnologici". "Il tema della cybersecurity non può più essere considerato esclusivamente sotto il profilo tecnico-informatico – dichiarano i consiglieri delegati Fabrizio Escheri ed Eliana Quintili –. La crescente digitalizzazione dei processi aziendali e l'evoluzione della disciplina dei reati informatici impongono di integrare il rischio cyber nei Modelli di organizzazione, gestione e controllo previsti dal d.lgs. 231/2001". Il documento approfondisce i principali reati informatici rilevanti ai fini del Dlgs. 231/2001, i profili organizzativi connessi all'integrazione del rischio cyber nei sistemi di compliance aziendale e il ruolo dell'Organismo di Vigilanza, anche alla luce dell'impatto delle nuove tecnologie e dell'intelligenza artificiale sui sistemi di controllo. Particolare attenzione è dedicata alla mappatura dei rischi e delle aree sensibili, all'aggiornamento dei protocolli e dei Codici Etici, alla formazione del personale e alle best practices in materia di cybersecurity. L'approfondimento proposto offre ai Commercialisti uno strumento di analisi e supporto operativo su un tema di crescente rilevanza per le imprese e per l'attività professionale.
Fonte: Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

LICENZIAMENTO ILLEGITTIMO SE LE RIPRESE VIDEO SENZA "FONDATO MOTIVO" E IN ASSENZA DI UN "FONDATO SOSPETTO"

Il licenziamento si considera illegittimo se le riprese video sul posto di lavoro vengono eseguite senza una reale necessità probatoria. Questo il principio espresso dalla Cassazione con ordinanza n. 16214/26. I Supremi giudici così sono tornati a pronunciarsi sul delicato tema dei controlli a distanza dei lavoratori e dell'utilizzabilità delle videoregistrazioni nei procedimenti disciplinari.
Gli Ermellini in particolare nella vicenda de quo hanno annullato con rinvio la sentenza della Corte d'Appello di Roma relativa al licenziamento di una dipendente di un supermercato di Guidonia Montecelio. La vicenda - Al centro della controversia vi sono le immagini registrate da telecamere installate all'interno del punto vendita tramite un'agenzia investigativa, utilizzate dal datore di lavoro per contestare alla dipendente numerosi episodi di consumo di prodotti alimentari senza pagamento e presunte violazioni delle norme igienico-sanitarie. La lavoratrice aveva impugnato il licenziamento sostenendo che le videoriprese fossero state effettuate in violazione dell'articolo 4 dello Statuto dei lavoratori (Legge 300/1970), che disciplina l'uso di impianti audiovisivi nei luoghi di lavoro. Secondo la difesa, l'installazione delle telecamere sarebbe avvenuta senza accordo sindacale né autorizzazione dell'Ispettorato del lavoro e in assenza di un "fondato sospetto" di illeciti specifici, condizione necessaria — secondo la giurisprudenza — per i cosiddetti "controlli difensivi".
La decisione di merito - La Corte d'Appello aveva dato ragione alla lavoratrice sul punto, ritenendo le immagini inutilizzabili perché acquisite al di fuori dei limiti di legge. Tuttavia, aveva comunque escluso il diritto al risarcimento, ritenendo che i fatti contestati risultassero sostanzialmente non contestati o confermati da altri elementi. La sentenza della Cassazione - Proprio su questo aspetto è intervenuta la Cassazione, che ha rilevato una contraddizione nella motivazione della sentenza d'appello: da un lato viene negata la validità probatoria delle videoriprese, dall'altro esse vengono di fatto utilizzate indirettamente per fondare la decisione su altri profili del giudizio (i profili risarcitori). La Suprema Corte, quindi, ha cassato la sentenza, disponendo un nuovo esame da parte della Corte d'Appello in diversa composizione, che dovrà rivalutare sia la legittimità delle videoriprese sia il loro eventuale valore probatorio nell'ambito del procedimento disciplinare.
Fonte: Il Sole 24 Ore - di Giampaolo Piagnerelli

USA: APPLE FORNIREBBE I CONTENUTI DELLE EMAIL RISERVATE ALLE AUTORITÀ FEDERALI

Negli Usa, Apple è al centro del dibattito perché avrebbe fornito alle autorità federali all'FBI le identità reali di almeno due utenti che avevano utilizzato una delle funzionalità pensate per proteggere la privacy. La funzione in questione, "Hide My Email", consente agli abbonati a iCloud+ di generare indirizzi e-mail anonimi, che inoltrano i messaggi verso la casella personale dell'utente senza rivelarne l'identità. Apple, da parte sua, ha sempre sostenuto di non leggere i contenuti delle e-mail inoltrate. Tuttavia, diversi documenti giudiziari hanno dimostrato che questa funzione non ha impedito alle Forze dell'ordine di risalire al proprietario di un indirizzo iCloud reso anonimo.
Secondo uno studio di TechCrunch, l'FBI ha richiesto informazioni ad Apple nell'ambito di un'indagine su un'email. La posta conteneva presunte minacce rivolte ad Alexis Wilkins, compagna del direttore dell'FBI Kash Patel. In risposta, la società ha confermato che "l'indirizzo utilizzato era un profilo anonimizzato associato a uno specifico Apple ID". I dati forniti includevano il nome completo dell'utente, l'indirizzo e-mail reale e informazioni relative a 134 indirizzi anonimi creati tramite la funzione "Hide My Email". Un secondo caso, sempre documentato da mandati di perquisizione, verteva su una richiesta avanzata da agenti federali dell'Homeland Security Investigations (HSI), unità interna all'ICE. Questo situazione, nell'ambito di un'indagine per frode d'identità. Anche in questo caso, Apple ha condiviso informazioni su un cliente sospettato, evidenziando la creazione di numerosi indirizzi di posta elettronica anonimizzati distribuiti su diversi profili. Sebbene Apple promuova gran parte dei servizi iCloud come "protetti da crittografia end-to-end" non tutte le informazioni risultano inaccessibili. Le autorità possono ottenere dati come nome, indirizzo, informazioni di fatturazione e contenuti non cifrati, tra cui le email, tramite specifiche procedure legali. Queste vicende hanno messo in luce i limiti strutturali della privacy nelle comunicazioni e-mail. "La maggior parte dei messaggi ancora oggi", hanno rimarcato gli esperti cyber, "non è protetta da crittografia end-to-end e contiene informazioni in chiaro necessarie per l'instradamento globale". Non sorprende quindi che "la domanda di applicazioni di messaggistica con crittografia completa sia in forte crescita". A spingere queste piattaforme è soprattutto l'esigenza di proteggere i dati personali, sia dalla sorveglianza istituzionale sia da attacchi informatici.
Fonte: CyberSecurity Italia

WHISTLEBLOWING, LICENZIAMENTO DEL SEGNALANTE? il carattere ritorsivo è presunto

Sentenza della sezione lavoro del Tribunale di Milano **n. 701 del 27 marzo 2026**

La disciplina fissata dalle disposizioni sul Whistleblowing (Dlgs. 24/2023) a tutela del soggetto che effettua una segnalazione si prolunga nell'eventuale giudizio che abbia ad oggetto la condotta (datoriale) vietata. Il legislatore ha scelto a tale scopo il meccanismo della inversione dell'onere della prova: non è al lavoratore/segnalante che spetta di provare il carattere ritorsivo del licenziamento ma è il datore di lavoro che deve dimostrare che il licenziamento è stato comminato per ragioni estranee alla segnalazione. A tal proposito merita attenzione la sentenza della sezione lavoro del Tribunale di Milano n. 701 del 27 marzo 2026, resa in una causa avviata con l'impugnazione del licenziamento.

Come da ricorso, il 9 dicembre 2024 il lavoratore aveva eseguito una segnalazione anonima tramite il canale interno, denunciando presunte irregolarità contrattuali e fiscali nella gestione di una commessa. Dopo l'audizione da parte del comitato interno competente per l'istruttoria, il successivo 17 dicembre egli era stato sollevato da tutte le attività senza alcuna comunicazione formale o motivazione. Appena due giorni dopo, il 19 dicembre, aveva ricevuto una lettera di contestazione disciplinare. Gli veniva contestata la presenza al lavoro in sede, negli ultimi 30 giorni, per n. 3 giorni soltanto, in violazione del limite massimo di giornate lavorate in smart working stabilito dagli accordi interni (60% su base settimanale). Inutilmente il lavoratore aveva risposto che detto utilizzo dello smart working rispondeva ad una prassi invalsa nel proprio gruppo di lavoro, senza che nessuno dei suoi colleghi fosse mai stato oggetto di rilievi disciplinari. Insoddisfatto della giustificazione, il datore lo aveva licenziato in tronco. Nel corso della fase istruttoria della causa di lavoro è emerso tramite l'escussione di vari testimoni che il superamento dei limiti dello smart working veniva effettivamente trattato con una certa tolleranza all'interno dell'azienda e che al massimo poteva essere stato oggetto di qualche rimprovero verbale.

Tutto questo ha messo in rilievo l'insussistenza della giusta causa del licenziamento. Dopodiché, valutate tutte le circostanze della contestazione disciplinare, ha potuto emergere il carattere meramente pretestuoso della contestazione stessa. Ai sensi del d.lgs. 24/2023, in particolare del suo art. 17, il segnalante non può subire alcuna ritorsione (comma 1); inoltre, in un qualunque procedimento giudiziario, amministrativo o relativo a controversia stragiudiziale che abbia ad oggetto l'accertamento dei comportamenti, atti o omissioni vietati nei confronti delle persone segnalanti, "si presume che gli stessi siano stati posti in essere a causa della segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile" (comma 2); ed ancora e quindi "l'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione, alla divulgazione pubblica o alla denuncia è a carico di colui che li ha posti in essere". Nella fattispecie, come affermato dal giudice, "tale onere non risulta assolto. La società resistente non ha fornito prova idonea a dimostrare che il licenziamento fosse determinato da ragioni autonome e indipendenti rispetto alla segnalazione effettuata dal ricorrente. Al contrario, l'istruttoria ha evidenziato come la prassi aziendale fosse di elasticità nella applicazione delle norme sul lavoro agile": da qui la pretestuosità della contestazione. Senonché gli indici di ritorsività non erano finiti lì e proprio "la concomitanza temporale tra segnalazione, estromissione del ricorrente dalle attività progettuali, contestazione disciplinare e licenziamento, unitamente all'infondatezza degli addebiti contestati", hanno consentito al giudice di ritenere che "la segnalazione abbia costituito il motivo determinante del recesso". Accertato l'intento ritorsivo del licenziamento, lo stesso è stato dichiarato nullo. Il lavoratore ha per conseguenza il diritto ad essere reintegrato nel posto di lavoro ed a percepire tutte le retribuzioni maturate dalla data del licenziamento a quella della effettiva reintegra, il tutto oltre interessi e rivalutazione monetaria.

LEGGI ON-LINE

Fonte: Articolo di Paolo Marini, Avvocato in Firenze

QUBIT

LAW FIRM & PARTNERS

Il partner legale per l'innovazione digitale

Chi Siamo

QUBIT Law Firm & Partners è una società tra avvocati, dove collaborano professionisti di vari settori per offrire consulenza altamente qualificata nel campo del diritto delle nuove tecnologie e dell'innovazione digitale.

Guidiamo l'innovazione, passo dopo passo

Supportiamo i nostri clienti in ogni fase dei loro progetti tecnologici e li aiutiamo ad affrontare le sfide poste dal mondo digitale. Il nostro approccio strutturato di Legal Project Management gestisce i progetti dalla fase di analisi alla realizzazione e governance, assicurando la conformità normativa fin dal primo momento.
Forniamo consulenza strategica per superare le complessità legali, tecniche e di business legate alla digitalizzazione.
La nostra mission è aiutare i nostri clienti a navigare nel panorama digitale, offrendo soluzioni su misura che combinano aspetti legali, di compliance e tecnici.

I nostri settori

- **Data Protection e GDPR Security**
- **Cybersecurity Law**
- **Intelligenza Artificiale e tecnologie innovative**
- **Identità Digitale e Soluzioni eIDAS 2**
- **FinTech, InsurTech, RegTech e Regolamentazione Bancaria e Finanziaria**
- **Contrattualistica**
- **Consulenza Societaria, Startup e Venture Capital**
- **Diritto Penale e Responsabilità Amministrativa degli Enti**

I soci di Qubit Law Firm & Partners

Avv. Massimiliano Nicotra
Dott. Giuseppe Giuliano
Avv. Savino Casamassima
Avv. Daria Alessi
Avv. Giulia Scarpino

Contattaci all'indirizzo info@qubitlawfirm.it o visita il nostro sito https://www.qubitlawfirm.it per scoprire come possiamo affiancarti

HIGH TECH LAW FIRM

TRASPARENZA SALARIALE e **PROTEZIONE** dei **DATI PERSONALI** con la Direttiva UE 2023/970

> ***Il decreto legislativo segna una profonda trasformazione nell'organizzazione del diritto del lavoro, modificando la trasparenza salariale in un modello di regolazione organizzativa e non più soltanto in uno strumento di tutela antidiscriminatoria***

L'approvazione definitiva, da parte del Consiglio dei Ministri del 30 aprile 2026, del decreto legislativo di recepimento della Direttiva UE 2023/970 rappresenta uno dei passaggi più significativi degli ultimi anni in materia di trasparenza salariale, in quanto la nuova disciplina non introduce un mero obbligo informativo aggiuntivo, ma modifica profondamente il rapporto tra organizzazione aziendale, sistemi retributivi, gestione delle risorse umane e tutela dei dati personali. Il vero elemento di discontinuità del nuovo quadro normativo consiste probabilmente nella trasformazione della retribuzione da elemento essenzialmente individuale del rapporto di lavoro in dato organizzativo regolato, divenendo oggi informazione che deve essere classificata, confrontata, documentata, verificata e, in alcuni casi, comunicata. Ciò comporta inevitabilmente una crescita esponenziale dei flussi informativi interni alle organizzazioni e una progressiva emersione di problematiche legate alla protezione dei dati personali.

Il legislatore europeo parte da una constatazione in fondo semplice, e cioè che le discriminazioni salariali persistono anche a causa dell'opacità dei sistemi retributivi, ed è per questa ragione che la Direttiva UE 2023/970 e il decreto legislativo nazionale di recepimento costruiscono un sistema complesso fondato sulla trasparenza, sulla tracciabilità delle decisioni organizzative e sulla verificabilità delle differenze salariali. Tuttavia, proprio mentre il sistema richiede maggiore conoscibilità delle informazioni economiche, emerge con forza l'opposto rischio della trasformazione della trasparenza salariale in una forma di circolazione incontrollata dei dati retributivi, dando così centrale risalto ai temi della riservatezza e della privacy. La nuova disciplina impone infatti alle organizzazioni una complessa operazione di bilanciamento tra esigenze solo apparentemente convergenti, quali quella di garantire effettività alla tutela antidiscriminatori e nel contempo di preservare la riservatezza delle informazioni economiche individuali. In questo scenario - i cui possibili effetti dannosi sono moltiplicati dal rapido diffondersi delle ormai note automazioni dovute alla massiva introduzione degli algoritmi nella gestione del rapporto di lavoro - anche la certificazione della parità di genere introdotta dalla legge n. 162/2021 va osservata in un'ottica diversa rispetto al passato, armonizzata con la nuova disciplina in oggetto e considerata non più soltanto strumento reputazionale o premiale, ma componente strutturale della governance aziendale e della compliance organizzativa. Il nuovo paradigma sulla trasparenza salariale - Come detto, il decreto legislativo approvato dal Governo il 30 aprile 2026 recepisce la Direttiva UE 2023/970 introducendo nel sistema italiano una disciplina destinata a incidere profondamente sulle modalità di gestione del personale.

Le nuove disposizioni, pienamente vincolanti sono dal giugno 2026, ma è evidente che i principi contenuti nel Decreto sono in larga parte immediatamente applicabili e che l'adeguamento organizzativo e l'implementazione delle relative misure richiederà tempi molto lunghi, posto che le imprese saranno chiamate a intervenire su procedure di selezione, sistemi di classificazione professionale, modelli retributivi, processi decisionali, infrastrutture HR e assetti documentali.

La trasparenza salariale non viene infatti più concepita come strumento eventuale di controllo successivo, ma come caratteristica strutturale dell'organizzazione. Tra le novità di maggiore impatto operativo vi è il diritto del candidato a conoscere il livello retributivo iniziale o la relativa fascia economica già nella fase preassuntiva perché la disposizione incide direttamente sulle tradizionali dinamiche negoziali che hanno storicamente caratterizzato il mercato del lavoro. Il legislatore europeo e quello nazionale mirano infatti a impedire che la posizione contrattuale del lavoratore sia influenzata da asimmetrie informative o da precedenti trattamenti discriminatori e coerentemente con questa impostazione, il Decreto vieta al datore di lavoro di richiedere informazioni sulle retribuzioni percepite nei precedenti rapporti di lavoro. Il sistema si accompagna inoltre a obblighi progressivi di reporting retributivo parametrati alla dimensione occupazionale dell'impresa e destinati a diventare progressivamente più stringenti, sino a imporre, nei casi di differenziali superiori al 5% non giustificati da fattori oggettivi e neutri, l'attivazione della procedura di valutazione retributiva congiunta prevista dal Decreto. La ratio della norma è evidentemente quella di evitare che eventuali discriminazioni storiche continuino a produrre effetti attraverso il trascinamento automatico delle condizioni economiche pregresse, ma dal punto di vista operativo si tratta di una previsione destinata a modificare significativamente le pratiche di recruiting e i processi di selezione e le organizzazioni aziendali dovranno ripensare modelli di colloquio, procedure HR e sistemi documentali, eliminando qualsiasi riferimento alle pregresse condizioni economiche del candidato. Ancor più delicata nella sua declinazione pratica è la previsione del diritto del lavoratore di ottenere informazioni sui livelli retributivi medi, distinti per sesso, relativi ai dipendenti che svolgono lo stesso lavoro o un lavoro di pari valore, ancorché proprio sul concetto di "lavoro di pari valore" il testo definitivo opera in realtà una delle scelte tecnicamente più interessanti, poiché la nozione viene raccordata ai sistemi di classificazione professionale previsti dalla contrattazione collettiva, al fine di utilizzarne la struttura classificatoria come strumento di neutralizzazione del rischio discriminatorio.

Il riferimento ai CCNL non svolge soltanto una funzione interpretativa, ma rappresenta piuttosto il tentativo del legislatore di costruire parametri comparativi oggettivabili e ridurre il rischio di arbitrarietà nei meccanismi di valutazione, tema questo della comparatività dei CCNL che in realtà caratterizza, trasversalmente e a vario titolo, la maggior parte dei più recenti interventi normativi in materia di lavoro, a cominciare dalla riforma delle previsioni sulla congruità del costo della manodopera introdotte nel D.lgs 36/2023 dal c.d. Correttivo appalti per finire poi con il recentissimo "Decreto 1° Maggio" n. 62/2026.

Trasparenza salariale e protezione dei dati personali - Come accennato poco sopra, il profilo probabilmente più delicato della nuova disciplina riguarda proprio il rapporto tra trasparenza salariale e tutela dei dati personali e della riservatezza del lavoratore. La concreta applicazione del decreto comporterà inevitabilmente un incremento massivo dei trattamenti di dati retributivi, nonché decisioni complesse sul bilanciamento di interessi tra quello del richiedente le informazioni sul trattamento retributivo altrui e il diritto alla riservatezza di detti soggetti.

Le organizzazioni saranno chiamate a raccogliere, classificare, aggregare e confrontare informazioni economiche sempre più dettagliate, spesso integrate con dati concernenti mansioni, percorsi professionali, sistemi incentivanti, valutazioni delle performance, progressioni di carriera e accesso alle posizioni di responsabilità.

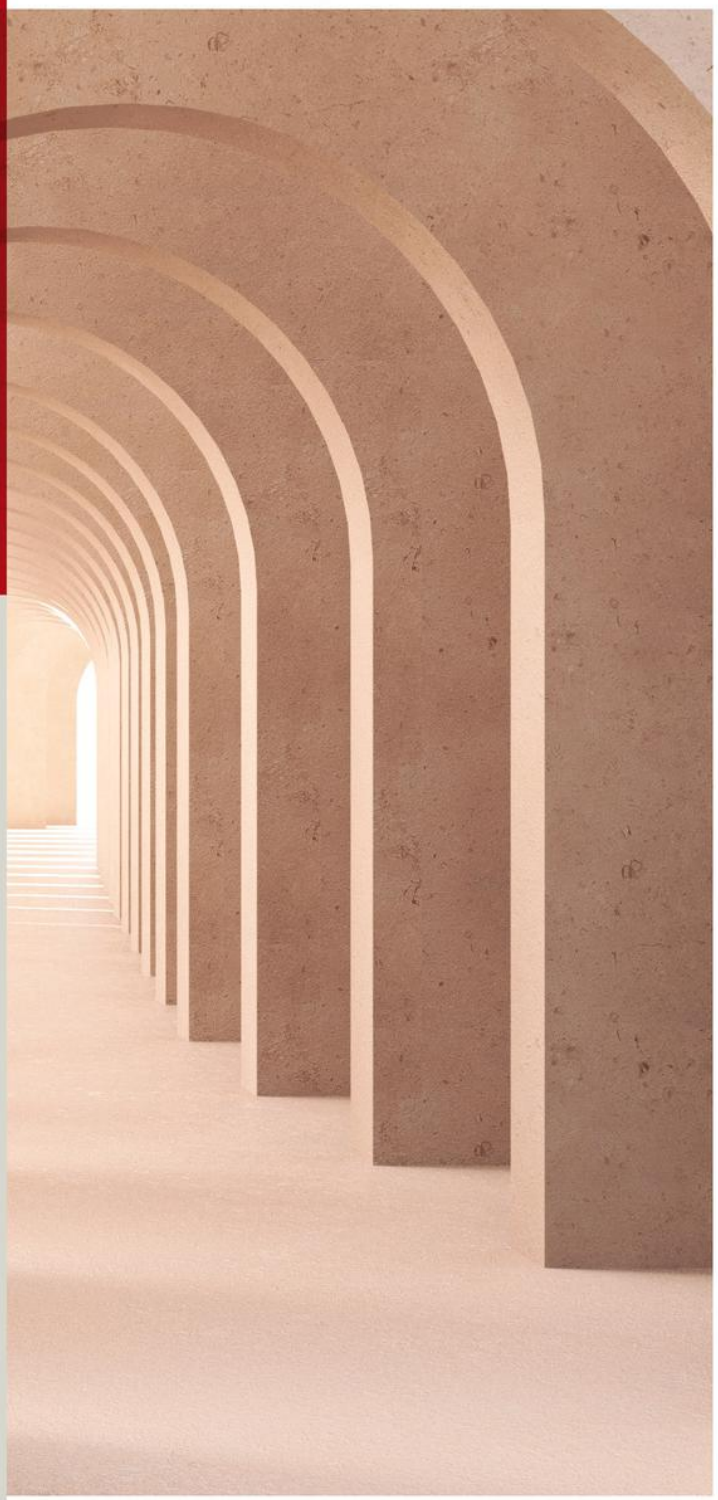
Pur non trattandosi, nella generalità dei casi, di categorie particolari di dati ai sensi dell'articolo 9 del GDPR, è evidente che le informazioni retributive incidono direttamente sulla dignità professionale e sulla sfera personale del lavoratore e come tali costituiscono pertanto dati la cui riservatezza è sicuramente di preminente rilievo, posto che il dato economico rappresenta una delle informazioni più sensibili nell'ambito delle relazioni organizzative.

.... continua a leggere online

APPROFONDIMENTO GRATUITO PER GLI UTENTI DEL SITO FEDERPRIVACY

Fonte: Il Sole 24 Ore
Articolo di Rafaele Sanna Randaccio

25 ANNI
Al servizio delle Organizzazioni.



La nostra affidabilità,
la tua efficienza!

- Protezione dei dati personali
- Responsabilità amministrativa D.Lgs. 231/01
- Whistleblowing
- Salute e sicurezza
- IORP 2
- Ambiente
- Sostenibilità
- Sistemi di Gestione
- DORA e NIS2
- Formazione

Compliance, Governance, Innovazione

PROTECTIONTRADE.IT

PROTECTION TRADE

2001•2026 25° ANNIVERSARIO

DIPENDENTI "CURIOSI": le **MISURE** organizzative necessarie per **PROTEGGERE** i **DATI AZIENDALI** ed evitare sanzioni del Garante Privacy

> Quasi **ogni organizzazione** convive con **sistemi di accesso ai dati** che, se sottoposti a un controllo rigoroso, rivelerebbero **criticità**

Un dipendente di filiale apre il gestionale. Digita il nome di un cliente — non suo, non della sua area, non per ragioni di lavoro. Lo fa per curiosità, o per qualcosa di peggio. Ripete questa operazione ben 6.637 volte nell'arco di due anni, senza che alcun sistema di controllo si attivi. Questo è la sintesi del caso Intesa Sanpaolo. L'aspetto sorprendente è che non si tratta di un attacco informatico sofisticato dall'esterno, ma di un "banale" accesso da parte di un "curioso" dotato di credenziali e privilegi, in assenza di un'adeguata supervisione. Il 26 marzo 2026 il Garante per la protezione dei dati personali ha emesso il Provvedimento n. 208, comminando a Intesa Sanpaolo S.p.A. una sanzione mostre di 31,8 milioni di euro. Il protagonista della vicenda è un dipendente della filiale Agribusiness di Barletta che, tra febbraio 2022 e aprile 2024, aveva fatto accesso senza alcuna giustificazione professionale ai dati bancari di migliaia di clienti — tra cui persone politicamente esposte, figure istituzionali e conoscenti privati. Il dipendente è attualmente indagato per accesso abusivo a sistemi informatici e tentato procacciamento di notizie concernenti la sicurezza dello Stato. «...Il modello operativo consentiva agli operatori di interrogare in piena circolarità l'intera base clienti, senza controlli idonei a prevenire e individuare accessi non giustificati...», così recita il provvedimento. Il fallimento non risiede nella condotta individuale del dipendente — che non è oggetto di alcuna sanzione da parte del Garante — bensì nell'inadeguatezza delle misure tecniche e organizzative, che hanno reso possibile tale comportamento in modo invisibile e prolungato nel tempo. Il sistema consentiva a qualunque operatore di filiale di interrogare l'intera base dati dei clienti della banca senza restrizioni (geografiche, operative, temporali). Un modello pensato per la flessibilità del day by day, non per la sicurezza.

Nessun alert veniva generato per ricerche anomale in termini di volume, frequenza o pertinenza rispetto al ruolo. Il risultato finale è che un singolo dipendente ha potuto curiosare in oltre tremila posizioni finanziarie nel silenzio dei sistemi di monitoraggio.

L'insider threat - La sicurezza informatica aziendale è storicamente orientata verso l'esterno: firewall, antivirus, MFA, VAPT, ecc. Soluzioni implementate per tenere fuori chi non deve entrare. Tuttavia, una quota significativa delle violazioni di dati aziendali non proviene dall'esterno, bensì dall'interno. L'agente di minaccia (insider) è rappresentato da dipendenti, collaboratori e consulenti, ovvero persone con accesso legittimo ai sistemi che utilizzano tale accesso in modo improprio. Il fenomeno viene definito insider threat e presenta caratteristiche diverse a seconda della motivazione. Ci sono gli insider malevoli, mossi da interesse economico, rancore o intenti di spionaggio. Ci sono gli insider negligenti, che condividono credenziali o lasciano sessioni aperte. E poi ci sono gli insider "curiosi" — forse la categoria più diffusa e meno discussa — che accedono a dati senza autorizzazione non per arrecare danno, ma per semplice curiosità: lo stipendio di un collega, la situazione finanziaria di un vicino, i movimenti di un personaggio pubblico. È un impulso umano diffuso. I sistemi devono essere progettati per contenerlo. I segnali d'allarme che avrebbero dovuto emergere - Con il senno di poi, la condotta del dipendente avrebbe dovuto generare numerosi alert. Sono segnali evidenti di anomalia le interrogazioni effettuate da un operatore di filiale su migliaia di clienti fuori dalla propria area di competenza, con una frequenza incompatibile con qualsiasi mansione ordinaria, nonché gli accessi a posizioni di persone politicamente esposte in assenza di attività di compliance correlate.

.... continua a leggere online

CONTINUA ON-LINE LA LETTURA

Fonte: Articolo di Monica Perego, Membro del Comitato Scientifico di Federprivacy

LA CONSULENZA PER OTTEMPERARE AL REGOLAMENTO UE 2016/679 ED ALLE LEGGI NAZIONALI

La responsabilità e l'obbligo della consapevolezza di chi tratta dati personali sono i presupposti fondamentali per la sicurezza dei cittadini UE.

La **InPrivacy** srl si pone al servizio dei soggetti che rivestono il ruolo di Titolari o di Responsabili del trattamento per affiancarli nel processo di ottemperanza al «Regolamento Europeo 2016/679 per la protezione delle persone fisiche con riguardo alla protezione dei dati personali, nonché alla libera circolazione di tali dati» (Gdpr) e alle leggi nazionali correlate.

Tutti i nostri professionisti e docenti, oltre ad avere già maturato esperienza pluriennale nella gestione del trattamento dati, hanno formazione universitaria di area tecnico-giuridica e specifica nella materia (Master e corsi di specializzazione, certificazioni di auditor e lead auditor nelle norme ISO e schemi proprietari sulla sicurezza dei dati e sui sistemi di gestione).

SIAMO A:

FIRENZE
PISTOIA | MILANO | BOLZANO
VERONA

INPRIVACY srl - Sede Legale ed Amministrativa: Via S. Andrea n°40 - 51100 PISTOIA
Centralino: Tel: +39 0573-26743 - Fax: +39 0573-25694
Email: info@inprivacy.it - www.inprivacy.it

10 2026	14	Privacy Day Forum 2026	Arezzo Fiere & Congressi
	23	Corso di alta formazione "Data Governance e compliance nella gestione delle risorse umane"	Formazione a distanza
	23	Webinar 'La governance dei dati delle risorse umane nell'era dell' intelligenza artificiale: gli impatti nel settore pubblico e privato'	Formazione a distanza
	23	Webinar 'La compliance privacy nella selezione del personale e nella gestione del rapporto di lavoro'	Formazione a distanza
	30	Webinar 'Il ruolo del Data Protection Officer con l'intelligenza artificiale e i diritti degli interessati in ambito di lavoro'	Formazione a distanza
	30	Webinar 'Riservatezza, whistleblowing, e tempi di conservazione dei dati in ambito di lavoro'	Formazione a distanza
11 2026	06	Webinar 'Trattamenti in ambito di lavoro effettuati da soggetti esterni e circolazione dei dati nelle imprese di gruppo'	Formazione a distanza
	06	Webinar 'Istruzione, formazione e aggiornamento del personale per la governance dei dati in conformità al GDPR'	Formazione a distanza
	13	Webinar 'Videosorveglianza e controlli in azienda tra esigenze di efficienza, tutela del patrimonio, e privacy dei lavoratori'	Formazione a distanza
	13	Webinar 'Decreto Trasparenza e sistemi automatizzati: gli impatti sulla privacy dei lavoratori'	Formazione a distanza
	20	Webinar 'Sicurezza dei trattamenti di dati dei lavoratori e gestione dei data breach'	Formazione a distanza
	20	Webinar 'Sindacati e tutela degli interessi dell'impresa nella gestione del personale'	Formazione a distanza
	27	Webinar 'Privacy e lavoro: informatica forense e aspetti penalistici'	Formazione a distanza
	27	Webinar 'Data governance delle risorse umane: progettazione e realizzazione del modello organizzativo'	Formazione a distanza

LEGGI GLI APPUNTAMENTI
ON-LINE

Federprivacy è la principale associazione in Italia il cui più importante scopo è radunare tutti i professionisti della privacy e della protezione dei dati, nonché tutti gli altri addetti ai lavori che si occupano di tali tematiche, come i consulenti della privacy, data protection officer e privacy officer. Anche coloro che aspirano ad acquisire una qualificazione nell'ambito della privacy possono beneficiare di tutti i vantaggi e le soluzioni riservate agli associati, per il migliore svolgimento delle proprie attività in conformità della legislazione vigente. Federprivacy è una associazione apolitica, aconfessionale, indipendente, senza scopo di lucro e le sue finalità sono le seguenti:

- **promuovere** con ogni mezzo la divulgazione, la conoscenza ed il rispetto delle normative vigenti in materia di privacy e protezione dei dati su tutto il territorio nazionale ed internazionale
- **assistere, rappresentare e tutelare** gli associati in tutte le sedi in cui siano coinvolti direttamente o indirettamente gli interessi collettivi degli associati
- **fornire** direttamente o indirettamente agli associati **servizi, prodotti, aggiornamenti, assistenza e informazioni su tematiche e problematiche** connesse alle loro attività inerenti la privacy e la protezione dei dati
- **fornire** agli associati linee guida ed orientamenti in materia di privacy e protezione dei dati da assumere ed adottare a livello collettivo
- **svolgere la funzione di osservatorio e di centro di ricerca** indirizzato a monitorare i fenomeni e le evoluzioni della privacy e della protezione dei dati
- **cooperare** con autorità, istituzioni, enti pubblici ed altre associazioni per conseguire la migliore interpretazione ed applicazione della normativa vigente in materia di privacy e protezione dei dati
- **perseguire e promuovere** l'attuazione di normative riguardanti il trattamento e la protezione di dati personali ed altre materie affini adeguate ai reali contesti socioeconomici nazionali ed internazionali, salvaguardando sempre il diritto fondamentale alla riservatezza dell' individuo
- **contribuire alla crescita tecnica e professionale** di tutti gli associati, anche mediante corsi di qualificazione, di aggiornamento e di specializzazione, l'istituzione di borse di studio
- **perseguire e promuovere** la valorizzazione e lo sviluppo delle professioni afferenti la privacy e la protezione dei dati
- redigere, aggiornare e far rispettare il proprio codice etico e deontologico e le proprie norme di autoregolamentazione
- svolgere in generale ogni attività, anche arbitrale, che sia nell'interesse degli associati.

PERCHÉ DIVENTARE SOCIO

Iscrivendoti a Federprivacy, entri a far parte della principale associazione di professionisti della privacy, e potrai:

- Ricevere l'**attestato di qualità** rilasciato da Federprivacy per distinguerti nello svolgimento della tua professione
- Ricevere la **newsletter settimanale** e le **circolari** per essere costantemente aggiornato
- Aggiornare la tua preparazione professionale con **formazione ad hoc, meeting e convegni**
- Ricevere **gratuitamente e in esclusiva il magazine** trimestrale Privacy News
- Accedere a **moduli, schemi, formule e check list**
- Consultare gratuitamente la **banca dati giuridica** in materia di privacy
- Pubblicare on line nel **Registro Soci** la tua **scheda personale** per una maggiore visibilità

DIVENTA SOCIO

INFORMAZIONI

Privacy News - Associazione Federprivacy

EDITORE & STAMPA - Associazione Federprivacy Codice Fiscale 94156260484 e Partita iva IT06413480481 - Sede Legale: Via Brunetto Degli Innocenti n. 2 - 50063 Figline Valdarno (FI) - Italy -Indirizzo postale: Via Brunetto Degli Innocenti n. 2 - 50063 Figline Valdarno (FI) - Italy - Testata registrata presso il Tribunale di Firenze Reg. N.5871 del 08.05.2012 - La rivista è stata chiusa in redazione a maggio 2026.
ABBONAMENTI - Privacy news è un magazine trimestrale edito dall'Associazione Federprivacy, che non è in vendita, ma viene distribuito, nonché reso disponibile nella versione sfogliabile sul sito www.federprivacy.org, in direct mailing, e spedito in omaggio a tutti i soci Federprivacy in regola con il pagamento delle quote associative annuali.

INFORMATIVA PRIVACY
1. **Titolare del Trattamento e DPO**

- Titolare: Associazione Federprivacy, Via Brunetto Degli Innocenti 2, 50063 Figline Valdarno (FI).
- Data Protection Officer (DPO): Avv. Marco Soffientini. Contatti: dpo@federprivacy.org o form sul sito www.federprivacy.org.

2. **Tipologia di Dati Trattati -** Dati anagrafici, fiscali ed economici necessari ai rapporti associativi; Non vengono trattati dati "particolari" (ex sensibili) o giudiziari; se necessario, verrà richiesto il consenso preventivo.
3. **Finalità e Base Giuridica del Trattamento I dati sono trattati per erogare i servizi richiesti, perseguire i fini associativi, adempiere a obblighi legali/fiscali e gestire i rapporti finanziari e commerciali -** Dati obbligatori (leggi/regolamenti): il rifiuto del conferimento comporta l'impossibilità di instaurare o proseguire il rapporto; Dati facoltativi: il mancato conferimento sarà valutato di volta in volta dall'Associazione.
4. **Modalità e Durata del Trattamento** - Il trattamento avviene con strumenti elettronici (sito web incluso), cartacei o telefonici, con misure idonee a garantire sicurezza e riservatezza. I dati sono conservati per tutta la durata del rapporto e anche successivamente per adempimenti di legge e finalità amministrative/commerciali.
5. **Ambito di Comunicazione e Diffusione** - I dati non sono diffusi a soggetti indeterminati, a eccezione della pubblicazione sul sito web – per obblighi di trasparenza legati alla Legge 4/2013 sulle associazioni professionali – del registro soci online (contiene: nome, cognome, eventuale ragione sociale, indirizzo e numero di iscrizione). Possono essere comunicati a soggetti determinati: Personale interno autorizzato; Soggetti terzi per obblighi di legge; Partner/organizzatori di eventi, corsi o congressi a cui l'utente sceglie di partecipare; Consulenti esterni, istituti di credito e spedizionieri (nei limiti delle finalità ausiliarie e con vincolo di riservatezza).
6. **Diritti dell'Interessato** - L'interessato può esercitare in ogni momento i seguenti diritti verso il Titolare:
Accesso: confermare l'esistenza dei dati, riceverne comunicazione intelligibile e conoscerne origine, finalità e modalità di trattamento; Rettifica: richiedere aggiornamento, correzione o integrazione; Cancellazione/Limitazione: ottenere la cancellazione, anonimizzazione o blocco dei dati non più necessari; Opposizione: opporsi per motivi legittimi al trattamento;
Reclamo: diritto di promuovere reclamo all'Autorità Garante per la protezione dei dati personali.
Per consultare l'informativa privacy completa e per maggiori dettagli sui trattamenti eseguiti, si invita a visitare la pagina web dedicata all'indirizzo https://www.federprivacy.org/associazione/informativa-privacy.

UNO PER TUTTI, TUTTI PER UNO

KONSENTO

Konsento, grazie ad un flusso gestito sulle finalità, semplice ed immediato, permette anche agli operatori non esperti di GDPR di costruire e gestire in sicurezza qualsiasi tipologia di campagna marketing e di attività grazie al suo sistema innovativo chiamato Ipercubo.

FEATURES

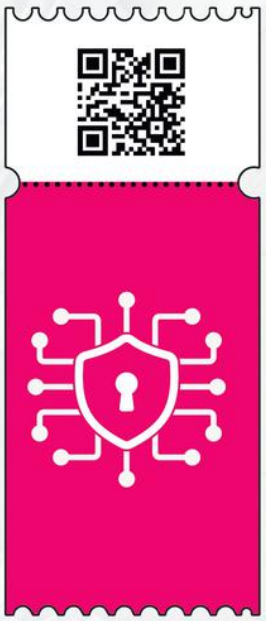
La gestione di consensi,
Le multifinalità,
La tracciatura immediata della corretta base giuridica nel luogo e nel tempo .
La puntualità delle informazioni trattate inerenti alla finalità gestita,
La multi liceità agganciata alle medesime finalità,
La gestione dei diritti degli Interessati

PRIVACYLAB
WE ARE WARRANT HUB
Warrant Hub S.p.A.
Società soggetta alla Direzione e Coordinamento di Tinexta S.p.A.
Sede operativa: Via del Fante, 45 - 42124 Reggio Emilia, Italia
Sede legale: Corso Mazzini, 11 - 42015 Correggio (RE), Italia
Tel. +39 0522 215092

inveo
ACADEMY

Compliance Learning Pass

L'abbonamento annuale che evolve con la compliance e integra privacy, cybersecurity, AI governance e molto altro...



Perchè scegliere il Compliance Learning Pass

- Aggiornamento continuo sulle evoluzioni normative per 365 giorni
- Percorso strutturato e coerente nel tempo
- Approccio integrato a privacy, cybersecurity e AI governance
- Flessibilità: il Pass può essere assegnato secondo le esigenze
- Continuità e valorizzazione delle competenze in azienda

3 livelli di accesso

Full Access Experience Pass

Il percorso più completo per chi necessita di una visione strategica e trasversale della compliance, grazie all'accesso integrale a tutti i moduli formativi.

Professional Pass

Destinato ai professionisti che presidiano quotidianamente i processi di compliance e desiderano mantenere un livello di competenza costantemente aggiornato.

Specialist Pass

Pensato per chi ha esigenza di focalizzarsi su temi specifici attraverso un percorso mirato e ad alta densità tecnica.

Vuoi saperne di più?

Scansiona il QR Code

formazione@in-veo.com

www.in-veo.com/academy

inveo
ACADEMY