

Aggiornamento Data protection, AI, IT and IP

n. 13 / 2024

DATA PROTECTION.

22 Ottobre 2024 – Garante privacy: la sistematica conservazione delle e-mail dei lavoratori e dei log di accesso alla posta elettronica e al gestionale aziendale per periodi di tempo sproporzionati è illecita.

INTELLIGENZA ARTIFICIALE.

18 Ottobre 2024 – Prospettive regolatorie della proposta di Direttiva sulla responsabilità civile per danno da Intelligenza Artificiale.

MERCATI DIGITALI

24 Ottobre 2024 – Commissione UE: consultazione pubblica sul progetto di regolamento delegato sull'accesso ai dati nell'ambito della legge sui servizi digitali (Regolamento 2022/2065 – DSA).

18 Ottobre 2024 – Autorità per le Garanzie nelle Comunicazioni: attivo il Portale delle segnalazioni on line.

INFORMATION TECHNOLOGY

17 Ottobre 2024 – Commissione UE: NIS 2, adottate le prime norme di attuazione della direttiva sulla sicurezza delle reti.

16 Ottobre 2024 – Agenzia Nazionale per la Cybersicurezza: pubblicata la *road map* per l'implementazione graduale presso le imprese degli obblighi previsti dalla Direttiva NIS 2 e dal decreto legislativo di recepimento.

16 Ottobre 2024 – Corte Suprema di Cassazione: non è diffamazione se il mittente ignora che all'account Messenger hanno accesso più persone.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

25 Ottobre 2024 – Ministero delle Imprese e del Made in Italy: apertura dal 29 ottobre dello sportello per accedere ai finanziamenti del programma Brevetti+ 2024.



22 Ottobre 2024 – Ministero delle Imprese e del Made in Italy: rapporto anticontraffazione, in 9 mesi oltre 2.300 applicazioni della nuova Legge sul Made in Italy.

DATA PROTECTION

22 Ottobre 2024 – Garante privacy: la sistematica conservazione delle e-mail dei lavoratori e dei log di accesso alla posta elettronica e al gestionale aziendale per periodi di tempo sproporzionati è illecita.

La sistematica conservazione delle e-mail dei lavoratori - effettuata per un considerevole periodo di tempo (pari a tre anni successivamente alla cessazione del rapporto) – e la sistematica conservazione dei log di accesso alla posta elettronica e al gestionale utilizzato dai lavoratori risulta non proporzionata e necessaria al conseguimento delle finalità dichiarate dal datore di lavoro, cioè quelle di garantire la sicurezza della rete informatica e la continuità dell'attività aziendale.

Lo ha stabilito il Garante Privacy sanzionando una società per 80mila euro.

Per tali sproporzionate finalità il datore di lavoro non può accedere alla posta elettronica del dipendente o del collaboratore né utilizzare un software per conservare una copia dei messaggi. Un simile trattamento di dati personali, oltre a configurare una violazione della disciplina in materia di protezione dei dati personali, è idoneo a realizzare un'illecita attività di controllo del lavoratore.

Il Garante, intervenuto a seguito del reclamo presentato da un agente di commercio, ha accertato che la società nel corso del rapporto di collaborazione, attraverso un software, aveva effettuato un backup della posta elettronica, conservando sia i contenuti che i log di accesso alla e-mail e al gestionale aziendale. Le informazioni raccolte erano poi state utilizzate dalla società in un contenzioso.

L'Autorità ha appurato inoltre l'ineidoneità e la carenza dell'informativa resa ai lavoratori. Il documento prevedeva infatti la possibilità, per il datore di lavoro, di accedere alla posta elettronica dei propri dipendenti e collaboratori per garantire la continuità dell'attività aziendale, in caso di loro assenza o cessazione del rapporto, senza citare, tra l'altro, l'effettuazione del backup e il relativo tempo di conservazione.

Ciò, inoltre, aveva consentito alla Società di ricostruire, minuziosamente, l'attività del collaboratore, incorrendo così in una forma di controllo vietata dallo Statuto dei lavoratori.

Per quanto riguarda infine l'uso dei dati in tribunale, il Garante ricorda che il trattamento effettuato accedendo alla posta elettronica del dipendente per finalità di tutela in ambito giudiziario si riferisce a contenziosi già in atto, non ad ipotesi di tutela astratte e indeterminate come in questo caso.

Oltre alla sanzione, l'Autorità ha disposto il divieto di ulteriore trattamento dei dati attraverso il software utilizzato per il backup della posta elettronica.

INTELLIGENZA ARTIFICIALE.

18 Ottobre 2024 – Prospettive regolatorie della proposta di Direttiva sulla responsabilità civile per danno da Intelligenza Artificiale.

Nel settembre 2022 la Commissione europea ha presentato una proposta di direttiva sull'adeguamento delle norme sulla responsabilità civile extracontrattuale all'intelligenza artificiale (AILD). Sebbene il Parlamento europeo e il Consiglio abbiano concordato in modo informale il testo della proposta nel dicembre 2023, si prevede che il testo cambierà sulla base di una valutazione d'impatto complementare pubblicata dal Servizio di ricerca del Parlamento europeo a fine settembre 2024 e che ha individuato le principali carenze e proposto che la Direttiva estenda il suo campo di applicazione per includere i sistemi di IA di uso generale e altri "sistemi di IA ad alto impatto", nonché il software. Discute inoltre un quadro di responsabilità mista che bilancia la responsabilità basata sulla colpa e la responsabilità oggettiva.

La valutazione di impatto del Parlamento UE da ultimo svolta raccomanda la transizione da una direttiva incentrata sull'IA a una regolamentazione sulla responsabilità del software, per prevenire la frammentazione del mercato e migliorare la chiarezza in tutta l'UE.



La commissione giuridica del Parlamento europeo (JURI), responsabile dell'adozione della legislazione in materia di responsabilità dell'IA, dovrebbe decidere in queste settimane se seguire il suggerimento della valutazione d'impatto di abbandonare l'attuale proposta di direttiva e raccomandare alla Commissione europea di proporre un regolamento sulla responsabilità dell'IA.

Nel frattempo, il Consiglio UE ha inviato interrogazioni ai governi degli Stati membri su: i) le misure che i richiedenti dovrebbero adottare per identificare la persona potenzialmente responsabile dei danni; e ii) la presunzione relativa di un nesso casuale tra il sistema di IA e il danno in determinate circostanze.

MERCATI DIGITALI

24 Ottobre 2024 – Commissione UE: consultazione pubblica sul progetto di regolamento delegato sull'accesso ai dati nell'ambito della legge sui servizi digitali (Regolamento 2022/2065 – DSA).

La Commissione europea ha avviato una consultazione pubblica su un progetto di regolamento per l'accesso ai dati ai sensi del Digital Services Act (DSA), che impone alle piattaforme online di dimensioni molto grandi (VLOP) e ai motori di ricerca online di dimensioni molto grandi (VLOSE) di fornire dati a fini normativi, di ricerca e di valutazione della mitigazione dei rischi.

La bozza istituisce il *portale di accesso ai dati DSA* quale *entry point* centralizzato per lo scambio di informazioni, definisce i ruoli della Commissione in qualità di Titolare del trattamento e di coordinatore dei servizi digitali nella valutazione delle richieste di accesso di terzi (che devono essere motivate), tenendo conto del livello di confidenzialità dei dati e dei diritti dei soggetti che sono chiamati a fornirli.

Il regolamento specifica, inoltre, le condizioni per la fornitura di dati a ricercatori selezionati e il divieto di imporre determinati requisiti che potrebbero ostacolare la ricerca, pur consentendo limitazioni all'uso degli strumenti analitici. Il periodo di consultazione pubblica termina il 26 novembre 2024.

18 Ottobre 2024 – Autorità per le Garanzie nelle Comunicazioni: attivo il Portale delle segnalazioni on line.

Il 15 ottobre 2024 è entrato in funzione il [Portale delle segnalazioni](#) dell'Agcom, attraverso il quale gli utenti e i consumatori potranno inviare on line le segnalazioni all'Autorità in modo semplice e intuitivo: si tratta delle segnalazioni attualmente trasmesse all'Agcom mediante i Modelli D e P per le violazioni contrattuali e di legge commesse dai fornitori di servizi di comunicazioni elettroniche; media audiovisivi, pay-tv e postale.

Per accedere al sistema e inviare la segnalazione è necessario autenticarsi attraverso SPID, CIE, CNS oppure eIDAS, e compilare i nuovi form elettronici.

INFORMATION TECHNOLOGY

17 Ottobre 2024 – Commissione UE: NIS 2, adottate le prime norme di attuazione della direttiva sulla sicurezza delle reti.

La Commissione UE ha adottato le prime norme di attuazione sulla sicurezza informatica di entità e reti critiche ai sensi della direttiva sulle misure per un elevato livello comune di sicurezza informatica nell'Unione (direttiva NIS2).

Il regolamento attuativo specifica le misure di gestione del rischio di sicurezza informatica nonché i casi in cui un incidente dovrebbe essere considerato significativo a chi devono segnalarlo le aziende che forniscono servizi digitali e in quale lasso di tempo. Il regolamento attuativo si applicherà a specifiche categorie di aziende che forniscono servizi digitali, come i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i marketplace online, i motori di ricerca online e le piattaforme di social network. Per

ciascuna categoria di fornitori di servizi, viene specificato quando un incidente è considerato significativo, a chi deve essere segnalato e in quale lasso di tempo.

16 Ottobre 2024 – Agenzia Nazionale per la Cybersicurezza: pubblicata la *road map* per l'implementazione graduale presso le imprese degli obblighi previsti dalla Direttiva NIS 2 e dal decreto legislativo di recepimento.

La sicurezza informatica è sempre più importante per le imprese e le Pubbliche Amministrazioni. Dal 16 ottobre 2024 è applicabile la nuova normativa italiana sulla *Network and Information Security (NIS 2)*. Aumentano i campi di applicazione della normativa. I settori interessati diventano 18, di cui 11 altamente critici e 7 critici, coinvolgendo oltre 80 tipologie di soggetti, distinguendoli tra essenziali e importanti in relazione al livello di criticità delle attività svolte e del settore in cui operano. L'Agenzia per la cybersicurezza nazionale (ACN) è l'Autorità competente per l'applicazione della NIS 2 e punto di contatto unico, ed ha delineato in questi giorni un percorso graduale e sostenibile per consentire alle organizzazioni pubbliche e private di adempiere ai nuovi obblighi di legge.

Ciò alla luce dei maggiori obblighi per le misure di sicurezza e per la notifica degli incidenti e del maggiore potere di supervisione conferito all'ACN e agli organi preposti alla risposta agli incidenti e alla gestione della crisi. Previsti anche nuovi strumenti per la sicurezza informatica, come la divulgazione coordinata delle vulnerabilità, da realizzarsi attraverso la cooperazione e la condivisione delle informazioni a livello nazionale ed europeo.

L'adeguamento alla normativa NIS prevede un percorso sostenibile con una graduale implementazione degli obblighi.

Il primo passo, per i soggetti interessati, è quello di [registrarsi al portale di ACN](#). C'è tempo dal 1° dicembre 2024 fino al 28 febbraio 2025 per le medie e grandi imprese e, in alcuni casi, anche per le piccole e le microimprese.

Per agevolare il recepimento degli obblighi di notifica di incidente e delle misure di sicurezza, gli stessi verranno definiti in maniera progressiva e a valle delle consultazioni nell'ambito dei tavoli settoriali in seguito alle determinate del Direttore Generale di ACN che saranno adottate entro il primo quadrimestre del 2025.

È prevista, inoltre, una finestra temporale di implementazione differenziata: 9 mesi per le notifiche e 18 mesi per le misure di sicurezza, decorrenti dalla data di consolidamento dell'elenco dei soggetti NIS (fine marzo 2025).

Da aprile 2025 partirà quindi un percorso condiviso di rafforzamento della sicurezza informatica nazionale ed europea.

Per facilitare la comprensione delle novità, l'ACN ha pubblicato [un video](#) e delle [pagine informative](#).

16 Ottobre 2024 – Corte Suprema di Cassazione: non è diffamazione se il mittente ignora che all'account Messenger hanno accesso più persone.

Non integra il delitto di diffamazione (aggravata) l'invio di messaggi diffamatori attraverso la piattaforma *Messenger* quando l'uso di tale canale – nella convinzione del soggetto agente - non è pubblico ma si ritiene di interagire con un applicativo di messaggistica privata e di interloquire direttamente. L'imputato aveva diffuso al destinatario una missiva dal contenuto lesivo e diffamatorio, senza avere la consapevolezza che al dispositivo avessero accesso anche altri soggetti (tutti facenti parte di un'associazione a cui aderiva, in qualità di Presidente, anche la vittima). Tale circostanza rende assente il dolo poiché manca – secondo la Cassazione, che così ha statuito con la sua sentenza n. 36217/2024 - la consapevolezza della comunicazione "*con più persone*" richiesta dalla norma incriminatrice ai fini della sussistenza del dolo di diffamazione.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

25 Ottobre 2024 – Ministero delle Imprese e del Made in Italy: apertura dal 29 ottobre dello sportello per accedere ai finanziamenti del programma Brevetti+ 2024.

Dalle ore 12.00 del prossimo 29 ottobre, le micro, piccole e medie imprese potranno inviare le domande per accedere agli incentivi Brevetti+ 2024, l'intervento promosso dal Ministero delle Imprese e del Made in Italy per la valorizzazione economica dei brevetti, con una dotazione finanziaria pari a 20 milioni di euro.

Le agevolazioni, consistenti in un contributo a fondo perduto fino a un massimo di 140.000 euro e non superiore all'80% dei costi ammissibili, saranno concesse, in regime de minimis, anche alle PMI appena costituite, aventi sede legale e operativa in Italia, che possiedono almeno uno dei seguenti requisiti:

- essere titolari o licenziatari di un brevetto per invenzione industriale concesso in Italia successivamente al 1° gennaio 2023
- essere titolari di una domanda nazionale di brevetto per invenzione industriale depositata successivamente al 1° gennaio 2022 con un rapporto di ricerca con esito "non negativo"
- essere titolari di un brevetto concesso dall'EPO e convalidato in Italia successivamente al 1° gennaio 2023
- essere titolari di una domanda di brevetto europeo o di una domanda internazionale di brevetto depositata successivamente al 1° gennaio 2022, con un rapporto di ricerca con esito "non negativo" che rivendichi la priorità di una precedente domanda nazionale di brevetto.

L'agevolazione potrà raggiungere l'85% dei costi ammissibili nel caso di imprese in possesso della certificazione della parità di genere e il 100% per le imprese beneficiarie che al momento della presentazione della domanda risultano contitolari, con un Ente pubblico di ricerca, della domanda di brevetto o di brevetto rilasciato, ovvero titolari di una licenza esclusiva avente per oggetto un brevetto rilasciato a uno dei suddetti Enti pubblici, già trascritta all'UIBM, senza vincoli di estensione territoriali.

Il contributo è finalizzato all'acquisto dei seguenti servizi specialistici:

- progettazione, ingegnerizzazione e industrializzazione
- organizzazione e sviluppo
- trasferimento tecnologico

La misura è gestita da Invitalia per conto del Ministero delle Imprese e del Made in Italy.

22 Ottobre 2024 – Ministero delle Imprese e del Made in Italy: rapporto anticontraffazione, in 9 mesi oltre 2.300 applicazioni della nuova Legge sul Made in Italy.

A nove mesi dall'entrata in vigore della Legge "Made in Italy", sono 2.357 i casi concreti di applicazione delle nuove disposizioni normative anticontraffazione. Nello specifico, circa 100 sono i casi in cui è stata applicata la previsione relativa alla distruzione delle merci contraffatte sequestrate e oltre 2.200 i casi di applicazione delle nuove sanzioni pecuniarie, incrementate rispetto al passato.

Relativamente alle azioni di enforcement, nel primo semestre 2024 sono quasi 9.000 le operazioni di sequestro effettuate. In particolare, sono stati più di 2.700 gli interventi operati dalla Guardia di Finanza e oltre 4.000 quelli dell'Agenzia delle Dogane e dei Monopoli. Il Servizio Analisi Criminale del Ministero dell'Interno ha rilevato oltre 400 sequestri di beni a marchio contraffatto effettuati da Polizia di Stato, Carabinieri e Polizia Locale.

È quanto emerge dal [Rapporto Cnalcis](#), realizzato dalla Direzione Generale per la Proprietà Industriale – Ufficio Italiano Brevetti e Marchi del Mimit, sulle attività svolte per la lotta alla contraffazione dalle amministrazioni competenti. I dati sono stati presentati in occasione dell'avvio della nona edizione della Settimana Anticontraffazione 2024.

“Con la nuova normativa di stringe la morsa sul grave fenomeno della contraffazione. Siamo sulla strada giusta ma non dobbiamo mollare. Crescono infatti i rischi con la diffusione delle nuove tecnologie e dell’e-commerce, per questo massima attenzione a tutela del Made in Italy, priorità del nostro governo”, ha affermato il ministro Urso.

Nella Legge, infatti, sono state introdotte misure per la protezione dei marchi e delle eccellenze italiane, tramite il potenziamento delle sanzioni e l’ampliamento degli strumenti a disposizione delle autorità competenti.

A livello settoriale, prosegue il rapporto, l’agroalimentare è stato interessato da circa 300 interventi del MASAF-ICQRF e 35 dei Carabinieri (Comando per la Tutela Agroalimentare), di cui 26 a marchio tutelato DOP e IGP, 7 per privative vegetali e 2 relativi a Made in Italy. La tutela della salute ha visto, da parte dei Carabinieri – NAS, quasi 200 oscurazioni di siti web che vendevano prodotti sanitari falsi. Sono 1.200 le operazioni svolte, infine, dai Carabinieri per la tutela del patrimonio culturale.

Importante anche l’impegno istituzionale per prevenire e contrastare la diffusione del mercato del falso online: 7 sono le piattaforme web con cui si è consolidata la rete di collaborazione pubblico-privata, con la condivisione di intenti comuni per azioni e strumenti di rimedio.

Numerose le azioni per sensibilizzare i consumatori, soprattutto i giovani: oltre 3.000 gli studenti coinvolti quest’anno nella quarta edizione della “Giornata della Lotta alla Contraffazione per gli Studenti”; varie le attività formative svolte, anche grazie a webinar, per raggiungere il maggior numero di persone; 2 campagne anticontraffazione e 6 eventi durante la Settimana Anticontraffazione 2024.

Altro target centrale nelle azioni per la tutela, anche all’estero, della Proprietà Industriale sono le imprese: la Linea Diretta Anticontraffazione dedicata ha raccolto 447 segnalazioni di possibili violazioni dei diritti di Proprietà Industriale.

Anche per il 2023, l’Ufficio Italiano Brevetti e Marchi del Mimit ha elaborato nel database IPERICO oltre 500 mila dati, pervenuti dalle diverse banche dati delle autorità italiane di enforcement. Le principali evidenze emerse per il 2023 registrano che le categorie merceologiche maggiormente sequestrate per contraffazione sono state l’abbigliamento (43,2%), gli accessori per abbigliamento (23%) e le calzature (10,5%), tutti settori storicamente colpiti dal business illegale e che rappresentano alcune tra le produzioni di eccellenza della manifattura e del Made in Italy. Quanto alla provenienza degli articoli falsi, risulta prevalere la Cina, seguita da Turchia, Marocco e Pakistan.

Tra il 2008 e il 2023, sono stati quasi 241 mila i sequestri e 699,5 milioni i pezzi contraffatti sequestrati, per un valore economico stimato della merce sequestrata di oltre 6,14 miliardi di euro sottratti al circuito illegale.