FIVERS

Aggiornamento
Data protection, AI, IT e IP

n. 4 / 2024

DATA PROTECTION

17 Giugno 2024 – Garante privacy: pubblicato il provvedimento di indirizzo definitivo sul trattamento e la conservazione dei metadati della posta elettronica di lavoratori pubblici e privati.

---

13 Giugno 2024 – Commissione UE: pubblicato il rapporto sul GDPR del Multistakeholder Expert Group.

---

12 Giugno 2024 - Autorità Garante per la protezione dei dati personali: parere favorevole sullo schema di Regolamento per le infrastrutture digitali e per i servizi cloud della PA predisposto dall'Agenzia per la cybersicurezza nazionale (ACN).

---

12 Giugno 2024 – Autorità Garante per la protezione dei dati personali: rilasciate le FAQ che chiariscono presupposti giuridici e modalità del trattamento da parte degli Istituti di ricovero e cura a carattere scientifico (IRCCS) dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca.

---

6 Giugno 2024 – Corte europea dei Diritti Umani (CEDU): viola l'articolo 8 della Convenzione sui Diritti Umani il giudice che estrae i dati personali dal cellulare dell'avvocato.

INTELLIGENZA ARTIFICIALE.

18 Giugno 2024 – OCSE: pubblicato il rapporto sull'impiego dell'Intelligenza Artificiale nel settore pubblico e del governo statale.

---

13 giugno 2024 – I Presidenti del Parlamento e del Consiglio UE hanno firmato il Regolamento europeo sull'Intelligenza Artificiale.

---

10 Giugno 2024 – Unione europea: accessibili sul portale Open Data oltre 1,7 milioni di dati pubblici ad alto valore per l'addestramento dell'Intelligenza Artificiale mediante dataset di qualità.

MERCATI DIGITALI.

5 Giugno 2024 – Autorità Garante della Concorrenza e del Mercato – AGCM: sanzione di 3,5 milioni a Meta per pratiche commerciali scorrette.

INFORMATION TECHNOLOGY

11 Giugno 2024 – IL Governo italiano approva il decreto legislativo di recepimento della Direttiva 2022/2555 (NIS 2) relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (NIS 1).

PROPRIETA' INDUSTRIALE

5 Giugno 2024 – Tribunale UE: la McDonald's perde il marchio dell'Unione europea "*Big Mac*" per i prodotti a base di pollame.

DATA PROTECTION

17 Giugno 2024 – Garante privacy: pubblicato il provvedimento di indirizzo definitivo sul trattamento e la conservazione dei metadati della posta elettronica di lavoratori pubblici e privati.

A seguito della consultazione pubblica avviata dal Garante privacy sul documento di indirizzo "*Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati*", il 6 giugno la medesima Autorità ha emanato il documento definitivo con le indicazioni modificate ai datori di lavoro pubblici e privati, ricordando comunque che "*stante la natura orientativa del documento di indirizzo, dallo stesso non discendono nuovi adempimenti o responsabilità*".

Il Garante chiarisce meglio cosa si intende per "metadati" ai fini del documento di indirizzo: essi corrispondono tecnicamente alle informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica (MTA = Mail Transport Agent) e dalle postazioni nell'interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client (le postazioni terminali che effettuano l'invio dei messaggi e che consentono la consultazione della corrispondenza in entrata accedendo ai mailbox elettroniche, definite negli standard tecnici quali MUA – Mail User Agent).

Tali informazioni relative alle operazioni di invio e ricezione e smistamento dei messaggi possono comprendere gli indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati e, in certi casi, in relazione al sistema di gestione del servizio di posta elettronica utilizzato, anche l'oggetto del messaggio spedito o ricevuto. I metadati cui ci si riferisce nel documento (sia quelli di origine prettamente tecnica sia quelli, come il campo "Oggetto", determinati dagli utenti) presentano poi la caratteristica di essere registrati automaticamente dai sistemi di posta elettronica, indipendentemente dalla percezione e dalla volontà dell'utilizzatore. Infine, il provvedimento chiarisce che i metadati non vanno confusi con le informazioni contenute nel corpo del messaggio e-mail, anche quando sono informazioni tecniche in esso integrate o rappresentano l'insieme delle intestazioni tecniche strutturate che documentano l'instradamento del messaggio, la sua provenienza e altri parametri tecnici. Le informazioni contenute nell'***envelope***, ancorché corrispondenti a metadati registrati automaticamente nei log dei servizi di posta, sono inscindibili dal messaggio di cui fanno parte integrante che rimane sotto l'esclusivo controllo dell'utente (sia esso il mittente o il destinatario dei messaggi).

Venendo alle indicazioni utili ai titolari del trattamento per una corretta accountability, il Garante chiarisce che l'attività di raccolta e conservazione dei soli metadati/log necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica, rientra nell'articolo 4, comma 2 dello Statuto dei Lavoratori (non necessitando dunque l'accordo sindacale o l'autorizzazione) se il periodo di conservazione non supera i 21 giorni. L'eventuale conservazione per un termine ancora più ampio potrà essere effettuata, solo in presenza di particolari condizioni che ne rendano necessaria l'estensione, comprovando adeguatamente, in applicazione del principio di accountability previsto dall'art. 5, par. 2, del GDPR, le specificità della realtà tecnica e organizzativa del titolare. Diversamente, la generalizzata raccolta e la conservazione dei log di posta elettronica, per un lasso di tempo più esteso, potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori, richiede l'esperimento delle garanzie previste dall'art. 4, comma 1, della L. n. 300/1970.

---

13 Giugno 2024 – Commissione UE: pubblicato il rapporto sul GDPR del *Multistakeholder Expert Group.*

Il Multistakeholder Expert Group, il gruppo di esperti della Commissione UE sul regolamento generale sulla protezione dei dati (GDPR) ha pubblicato il suo rapporto sull'applicazione del GDPR.

Vi sono stati sviluppi positivi, tra cui un aumento della conformità dei trattamenti UE alle regole sulla protezione dei dati e della consapevolezza degli aventi diritto, oltre a maggiori controlli effettuati dalle persone fisiche sul trattamento dei loro dati. Il rapporto ha anche evidenziato un maggiore ricorso al diritto di accesso e al diritto alla cancellazione, ma ha rilevato che c'è ancora mancanza di consapevolezza tra

gli interessati sui loro diritti e su come esercitarli nella pratica, soprattutto per quanto riguarda il diritto di non essere soggetti a un processo decisionale automatizzato ai sensi dell'articolo 22 del GDPR.

Sempre in tema di attuali scenari circa l'esercizio dei diritti *data protection*, per quanto riguarda il diritto alla portabilità dei dati, il rapporto ha suggerito che la mancanza di consapevolezza circa il diritto alla portabilità dei dati è dovuta alla potenziale assenza di standardizzazione dei formati dei dati e al potenziale rischio che nel trasferire i dati a un'altra organizzazione possano esservi limitazioni o impatti sui diritti e sulle libertà fondamentali.

Quanto alla applicazione dei principi di protezione dei dati ai sensi del GDPR, criticità sono state rilevate circa i principi di minimizzazione dei dati e di limitazione dei tempi di conservazione. Sul principio di trasparenza, il rapporto ha evidenziato le preoccupazioni di molte organizzazioni, in particolare circa i rischi di impiego di termini vaghi o troppo complicati considerati non in linea con il GDPR.

Una particolare criticità è inoltre emersa circa il rapporto tra l'applicazione del GDPR e altri regolamenti o direttive della UE, come quelli relativi gli obblighi antiriciclaggio (AML) o la direttiva sui servizi di pagamento (PSD2). In questa prospettiva, il rapporto ha anche evidenziato la necessità di una maggiore chiarezza sull'interazione tra il GDPR e la prossima legge dell'UE sull'intelligenza artificiale (AI Act).

Anche l'adozione delle nuove clausole contrattuali standard (SCC) per i trasferimenti di dati a titolari e responsabili del trattamento al di fuori dell'UE il cui trattamento è soggetto al GDPR è un punto che il rapporto ha rilevato come critico a causa dell'ambiguità giuridica relativa ai requisiti applicabili che non sono ancora stati precisati da linee guida del Comitato europeo per la protezione dei dati (EDPB). La questione è ulteriormente complicata dai pareri potenzialmente contrastanti emessi dalle autorità nazionali di protezione dei dati sui trasferimenti transfrontalieri e dalla mancanza di coordinamento tra dette autorità, con differenze nelle procedure nazionali che hanno portato a decisioni incoerenti.

---

12 Giugno 2024 - Autorità Garante per la protezione dei dati personali: parere favorevole sullo schema di Regolamento per le infrastrutture digitali e per i servizi cloud della PA predisposto dall'Agenzia per la cybersicurezza nazionale (ACN).

Lo schema di Regolamento, che sostituisce l'atto adottato in precedenza dall'Agenzia per l'Italia digitale (AGID), tiene conto delle indicazioni fornite dal Garante nel corso delle interlocuzioni. Il documento introduce un nuovo articolo dedicato alla corretta applicazione della normativa privacy, che mira ad assicurare il controllo, da parte delle Pubbliche Amministrazioni, su tutti i soggetti che intervengono nel trattamento dei dati. In particolare, attribuisce alle PA il ruolo di titolari del trattamento, mentre gli operatori di infrastrutture digitali e i fornitori di servizi cloud vengono indicati quali responsabili del trattamento.

Il testo stabilisce inoltre l'obbligo per i responsabili del trattamento di adottare misure che garantiscano una tempestiva e adeguata informazione da parte delle amministrazioni in caso di data breach, considerata la mole e la delicatezza dei dati trattati (dati sulla salute, dati fiscali). I responsabili del trattamento dovranno poi fornire alle PA idonei strumenti di controllo delle attività di trattamento effettuate da eventuali sub responsabili.

In tema di trasferimenti dei dati al di fuori dello Spazio economico europeo, i responsabili del trattamento saranno tenuti ad attenersi alle istruzioni delle amministrazioni e a mettere a disposizione delle stesse ogni informazione necessaria per valutare l'effettività delle misure adottate.

Il Regolamento si inserisce all'interno della Strategia cloud Italia, messa in campo dal Dipartimento per la trasformazione digitale e da ACN, che contiene gli indirizzi per il percorso di migrazione verso il cloud di dati e servizi digitali della Pubblica Amministrazione, anche grazie al Polo Strategico Nazionale (PSN), quale infrastruttura cloud realizzata su impulso del governo.

---

12 Giugno 2024 – Autorità Garante per la protezione dei dati personali: rilasciate le FAQ che chiariscono presupposti giuridici e modalità del trattamento da parte degli Istituti di ricovero e cura a carattere scientifico (IRCCS) dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca.

Cosa sono gli IRCCS? Come possono utilizzare i dati personali raccolti per la cura dei pazienti per finalità di ricerca? A quali adempimenti sono tenuti in base al Codice privacy? A queste domande ha risposto il Garante Privacy con le apposite FAQ.

I chiarimenti dell'Autorità sono rivolti agli IRCCS, ossia quegli enti del Servizio sanitario nazionale che, secondo standard di eccellenza, perseguono finalità di ricerca nel campo biomedico e in quello dell'organizzazione e gestione dei servizi sanitari ed effettuano prestazioni di ricovero e cura di alta specialità.

Nelle FAQ è spiegato che gli IRCCS, per poter utilizzare i dati dei loro pazienti anche per l'attività di ricerca scientifica autorizzata dal Ministero, devono individuare una base giuridica idonea a legittimare tale trattamento e una deroga adeguata al generale divieto di trattare i dati sulla salute e genetici.

Il Garante ha dunque chiarito che gli IRCCS pubblici e privati, oltre che sul consenso dei partecipanti alla ricerca, possono fondare il trattamento dei dati personali raccolti a scopo di cura per ulteriori finalità di ricerca sull'art. 110-bis, comma 4 del Codice privacy, in base al quale non costituisce trattamento ulteriore dei dati raccolti per l'attività clinica, quello svolto a fini di ricerca.

Nel caso in cui gli IRCCS si avvalgano di questa disposizione, hanno però l'obbligo di svolgere la Valutazione d'impatto (DPIA) e di pubblicarla sui propri siti web. Tuttavia, se la pubblicazione per intero della DPIA può ledere diritti di proprietà intellettuale, segreti commerciali o altro, l'Istituto può pubblicarla per estratto.

Una specifica sezione delle FAQ è dedicata alle diverse le modalità per informare i partecipanti alla ricerca a seconda che i dati siano raccolti presso di essi ovvero presso banche dati interne all'istituto o altri centri partecipanti.

L'Autorità ha infine chiarito l'ambito oggettivo di applicazione dell'art. 110-bis, comma 4 del Codice, che riguarda ogni tipo di ricerca medica, biomedica, epidemiologica, prospettica e retrospettiva, promossa da IRCCS, ivi inclusi gli studi multicentrici, sia svolti nell'ambito delle reti di ricerca degli IRCCS che in quelli promossi da tali istituti con la partecipazione di enti che non godono di tale riconoscimento.

---

12 Giugno 2024 - Autorità Garante per la protezione dei dati personali: nei concorsi pubblici le Pubbliche Amministrazioni possono pubblicare on line solo le graduatorie definitive dei vincitori, pena la diffusione illecita di dati personali.

Pubblicare sul web gli esiti delle prove intermedie o dei dati personali dei concorrenti non vincitori o non ammessi ad un concorso è una violazione della privacy.

Così si è espresso il Garante a seguito di un reclamo presentato da un partecipante al concorso pubblico, a 1858 posti di consulente protezione sociale nei ruoli del personale dell'INPS.

Il reclamante aveva lamentato la pubblicazione sul sito web dell'Istituto di numerosi atti e documenti, tra cui gli elenchi degli ammessi e non ammessi alla prova scritta e prova orale e l'elenco dei partecipanti, contenente la valutazione dei titoli da parte della Commissione di concorso, con l'indicazione del punteggio attribuito a ciascun candidato. Tali documenti sarebbero poi finiti anche sui social network ad opera di terzi.

I soggetti pubblici, ha ricordato il Garante, quando operano nello svolgimento di procedure concorsuali devono trattare i dati personali degli interessati nel rispetto delle norme di settore applicabili, e quindi non è possibile pubblicare online dati dei partecipanti ai concorsi non previsti dalla legge. Non sono infatti consentiti livelli differenziati di tutela della protezione dei dati personali, né su base territoriale né a livello di singola amministrazione, specie quando la materia sia già stata oggetto di bilanciamento e regolazione dal legislatore con disposizioni uniformi a livello nazionale.

Nel quantificare l'importo della sanzione all'INPS in 20.000 euro l'Autorità ha considerato la natura, la durata e la gravità della violazione, nonché l'elevato numero degli interessati e l'atteggiamento collaborativo dell'Istituto, che ha rimosso gli elenchi in questione, seppur a seguito della richiesta di informazioni del Garante.

---

6 Giugno 2024 – Corte europea dei Diritti Umani (CEDU): viola l'articolo 8 della Convenzione sui Diritti Umani il giudice che estrae i dati personali dal cellulare dell'avvocato.

Il caso riguarda la conduzione di un'indagine giudiziaria da parte di un magistrato francese distaccato presso i tribunali monegaschi. La ricorrente è un avvocato un cui cliente è stato dalla stessa accusato di aver registrato di nascosto una conversazione durante un pasto privato. Dopo aver denunciato il reato di violazione della privacy, la ricorrente ha consegnato il suo telefono cellulare alla polizia in modo che la registrazione del reato potesse essere esaminata e la sua buona fede provata.

Il giudice istruttore, che era stato investito solo del compito di verificare l'autenticità della registrazione e l'esame del contenuto della conversazione alla luce del diritto penale monegasco, ha deciso invece di avviare un'indagine telefonica ad ampio raggio, senza alcuna reale limitazione in termini di tempo o di portata della ricerca, consentendo così di svolgere un'indagine "esplorativa".

La Corte EDU ha ritenuto che le indagini intraprese dal giudice istruttore sul telefono cellulare di un avvocato e il recupero massiccio e indiscriminato di dati personali, compresi quelli precedentemente cancellati, siano andati oltre l'ambito del mandato, che riguardava esclusivamente atti di violazione della privacy, e che tali indagini esorbitanti non siano state accompagnate da garanzie che rispettassero lo status di avvocato della ricorrente e il segreto professionale.

INTELLIGENZA ARTIFICIALE.

18 Giugno 2024 – OCSE: pubblicato il rapporto sull'impiego dell'Intelligenza Artificiale nel settore pubblico e del governo statale.

Con la pubblicazione del Rapporto *Governing with Artificial Intelligence: are governments ready*? l'OCSE rafforza la strategia - parte di uno sforzo più ampio - per fondare l'uso responsabile dell'IA nel settore pubblico, soprattutto in una serie di funzioni governative chiave. Il rapporto mira alla condivisione delle conoscenze, allo scambio di buone pratiche e al dialogo politico strutturato tra Stati membri per comprendere le implicazioni e orientare un uso responsabile dell'IA nel settore pubblico. IN questa prospettiva, mettere a disposizione dei governi maggiori e migliori indicatori e prove dell'impiego e dell'impatto dell'IA nell'azione amministrativa pubblica contribuirà a garantirne l'uso ottimale; inoltre, sarà necessario l'impegno di più parti interessate in tutti i settori politici e al di là dei confini nazionali per esplorare collettivamente le opzioni politiche man mano che emergono nuove sfide e opportunità.

È sempre più diffusa la consapevolezza che, se usata in modo strategico e responsabile, l'intelligenza artificiale (IA), compresa l'IA generativa, ha il potenziale per trasformare il modo in cui i governi funzionano, progettano le politiche e forniscono i servizi. I governi hanno molteplici ruoli in relazione all'IA, come promotori, finanziatori, regolatori, ma anche come utenti e, in alcuni casi, sviluppatori.

Mentre il dibattito globale sull'IA tende a concentrarsi sul ruolo dei governi come regolatori nel dare forma e risposta all'applicazione dell'IA, è stata prestata meno attenzione alle loro responsabilità come utenti dell'IA. Man mano che i governi colgono le opportunità offerte dall'IA per una migliore *governance* e

implementano soluzioni in un'ampia gamma di aree politiche, riconoscono la necessità di governare l'IA nel settore pubblico per prevenirne l'uso improprio e mitigarne i rischi.

In questo contesto, i Paesi dell'OCSE stanno investendo sempre più nella comprensione dei sistemi di IA e nell'utilizzo delle opportunità che essi offrono per trasformare la macchina amministrativa e cogliere le opportunità che offrono per trasformare l'apparato di governo.

L'uso responsabile dell'IA può migliorare il funzionamento delle amministrazioni pubbliche in diversi modi.

In primo luogo, l'uso dell'IA nel settore pubblico può aiutare i governi ad aumentare la produttività con amministrazioni più efficienti e politiche pubbliche più efficaci.

In secondo luogo, l'IA può contribuire a rendere la progettazione e l'erogazione di politiche e servizi pubblici più inclusivi e rispondenti alle esigenze in evoluzione dei cittadini e di specifiche comunità.

In terzo luogo, l'IA può rafforzare la responsabilità dei governi migliorando la loro capacità di controllo e sostenendo istituzioni di controllo indipendenti.

Questo potenziale non è stato ancora pienamente esplorato e sfruttato. Sono necessarie maggiori prove sui casi d'uso per capire meglio come sviluppare e implementare con successo le iniziative di IA, imparando dai successi e dai fallimenti. Nonostante i potenziali benefici dell'IA, crescono anche le preoccupazioni per i rischi di una diffusione frammentata e non governata dell'IA nel settore pubblico. Tali rischi includono l'amplificazione dei di pregiudizi, la mancanza di trasparenza nella progettazione dei sistemi e le violazioni della privacy e della sicurezza dei dati, tutti elementi che potrebbero portare a output ingiusti e discriminatori, con profonde implicazioni sociali.

Il settore pubblico ha una responsabilità particolare nell'impiegare l'IA in modo da ridurre al minimo i danni e dare priorità al benessere degli individui e delle comunità, soprattutto quando l'IA viene impiegata in ambiti politici sensibili come l'applicazione della legge, il controllo dell'immigrazione, le prestazioni sociali e la prevenzione delle frodi. I governi si stanno gradualmente adoperando per creare un ambiente che consenta lo sviluppo, la diffusione e l'utilizzo dell'IA in modo sicuro e affidabile durante l'intero ciclo politico. Questi sforzi comprendono la definizione di obiettivi strategici, l'esplorazione di nuovi accordi istituzionali, lo sviluppo di strumenti politici (come standard, codici, linee guida) e di nuovi quadri normativi, nonché l'attrazione delle capacità necessarie per utilizzare l'IA in modo efficace ed efficiente nel settore pubblico.

---

13 giugno 2024 – I Presidenti del Parlamento e del Consiglio UE hanno firmato il Regolamento europeo sull'Intelligenza Artificiale.

Il Presidente del Parlamento europeo e il Presidente del Consiglio dell'Unione europea hanno firmato la Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate sull'intelligenza artificiale (l'Atto sull'IA). Si attende a questo punto sola la pubblicazione in Gazzetta del provvedimento, che entrerà in vigore 20 giorni dopo e sarà applicabile a diverse scadenze (tra 6 e 36 mesi dalla entrata in vigore).

L'AI Act si applicherà:

- ai fornitori che immettono sul mercato o mettono in servizio sistemi di intelligenza artificiale (IA) o che immettono sul mercato modelli di IA per uso generale (GPAI) nell'UE, indipendentemente dal fatto che tali fornitori siano stabiliti o situati nell'UE o in un Paese terzo;
- ai distributori di sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'UE;
- ai fornitori e distributori di sistemi di IA con sede o ubicati in un Paese terzo, quando l'output prodotto dal sistema di IA è utilizzato nell'UE;
- a importatori e distributori di sistemi di IA;
- produttori di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio;

- ai rappresentanti autorizzati di fornitori che non sono stabiliti nell'UE; e
- a persone interessate nell'UE.

La legge sull'IA adotta un approccio basato sul rischio e vieta alcune pratiche di IA, tra cui la manipolazione cognitiva del comportamento, il social scoring, l'IA per la polizia predittiva basata sulla profilazione e i sistemi che utilizzano dati biometrici per classificare le persone in base a categorie specifiche come razza, religione o orientamento sessuale.

Inoltre, la legge sull'IA classifica alcuni sistemi di IA come ad *alto rischio* e specifica i requisiti per tali sistemi, alcuni dei quali richiedono una valutazione dell'impatto sui diritti fondamentali.

La legge sull'IA regola anche i sistemi GPAI che saranno soggetti a requisiti limitati, ad esempio per quanto riguarda la trasparenza. Tuttavia, quelli che presentano rischi sistemici dovranno rispettare regole aggiuntive.

La legge sull'IA istituirà i seguenti organi di governo:
- un Ufficio per l'IA all'interno della Commissione per far rispettare le regole comuni in tutta l'UE (già operativo da gennaio 2024);
- un gruppo scientifico di esperti indipendenti;
- un comitato per l'IA con rappresentanti degli Stati membri per supportare la Commissione e gli Stati membri nell'applicazione coerente ed efficace della legge sull'IA; e
- un forum consultivo per le parti interessate che fornisca competenze tecniche al comitato per l'IA e alla Commissione.

Quanto alle sanzioni, l'AI Act prevede diverse soglie per le ammende, fissate come percentuale del fatturato annuo globale dell'azienda nell'esercizio finanziario precedente o come importo predeterminato, a seconda di quale sia il più alto. Le piccole e medie imprese (PMI) e le start-up sono soggette a sanzioni amministrative proporzionali. In particolare, il mancato rispetto del divieto delle pratiche di IA di cui all'articolo 5 della legge sull'IA è soggetto a sanzioni amministrative pecuniarie fino a 35 milioni di euro o, se il trasgressore è un'impresa, fino al 7% del suo fatturato mondiale totale annuo dell'anno finanziario precedente, a seconda di quale sia l'importo più alto.

---

10 Giugno 2024 – Unione europea: accessibili sul portale Open Data oltre 1,7 milioni di dati pubblici ad alto valore per l'addestramento dell'Intelligenza Artificiale mediante dataset di qualità.

Sono ufficialmente entrate in vigore le nuove regole dell'Ue per rendere disponibili per il riutilizzo – mediante il portale ufficiale raggiungibile qui - quasi 1,7 milioni di dati pubblici considerati "set di dati ad alto valore" su sei aree tematiche stabilite dalla direttiva sui dati aperti: geospaziale, osservazione della terra e ambiente, meteorologica, statistica, imprese e mobilità.

Tali dati potranno essere liberamente utilizzati per il machine learning dei sistemi di IA, promuovendo lo sviluppo di nuovi prodotti e servizi innovativi in quei settori.

MERCATI DIGITALI.

5 Giugno 2024 – Autorità Garante della Concorrenza e del Mercato – AGCM: sanzione di 3,5 milioni a Meta per pratiche commerciali scorrette.

L'Autorità Garante della Concorrenza e del Mercato ha sanzionato per 3,5 milioni di euro Meta Platforms Ireland Ltd. e la capogruppo Meta Platforms Inc. per due pratiche commerciali ingannevoli riguardo alla creazione e alla gestione degli account dei social network Facebook e Instagram.

L'Autorità ha accertato che Meta, in violazione degli articoli 20, 21 e 22 del Codice del consumo, non ha informato con immediatezza gli utenti iscritti ad Instagram via web dell'utilizzo dei loro dati personali per finalità commerciali.

Inoltre, l'Autorità ha appurato che, in violazione dell'articolo 20 del Codice del consumo, Meta non ha gestito con precisione la sospensione degli account Facebook e Instagram dei propri utenti. In particolare, Meta non ha indicato come decida di sospendere gli account Facebook (se a seguito di un controllo automatizzato o "umano") e non ha fornito agli utenti di Facebook e Instagram informazioni sulla possibilità di contestare la sospensione dei loro account (si possono rivolgere a un organo di risoluzione stragiudiziale delle controversie o a un giudice). Infine, ha previsto un termine breve (30 giorni) per la contestazione della sospensione da parte del consumatore.

INFORMATION TECHNOLOGY

11 Giugno 2024 – IL Governo italiano approva il decreto legislativo di recepimento della Direttiva 2022/2555 (NIS 2) relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (NIS 1).

La direttiva NIS2 è la legislazione dell'UE in materia di cibersicurezza. Esso prevede misure giuridiche per rafforzare il livello generale di cibersicurezza nell'UE. Rispetto alla precedente direttiva del 2016 (NIS 1) ha modernizzato il quadro giuridico esistente per tenere il passo con una maggiore digitalizzazione e un panorama in evoluzione delle minacce alla cibersicurezza, estendendo l'ambito di applicazione delle norme in materia di cibersicurezza a nuovi settori e entità e migliorando ulteriormente la resilienza e le capacità di risposta agli incidenti degli enti pubblici e privati, delle autorità competenti e dell'UE nel suo complesso.

La Direttiva NIS 2 introduce una rinnovata cultura della sicurezza in tutti i settori che sono vitali per l'economia e la società europea e che dipendono fortemente dalle Tecnologie dell'Informazione e Comunicazione (TIC), come l'energia, i trasporti, l'acqua, le infrastrutture bancarie e dei mercati finanziari (si ricordi che la NIS 2 non si applica ai soggetti bancari, finanziari e assicurativi tenuti al rispetto del Regolamento DORA 2022/2554 sulla resilienza operativa digitale, vera e propria *lex specialis* del settore), l'assistenza sanitaria e le infrastrutture digitali (i fornitori TIC sono anche soggetti al Regolamento DORA citato).

Il decreto legislativo italiano interviene introducendo le seguenti principali novità (il termine posto agli Stati Membri per il recepimento è il 17 ottobre 2024):

- l'ampliamento dell'ambito soggettivo di applicazione della disciplina;
- la distinzione tra "soggetti essenziali" e "soggetti importanti" e l'adozione di un criterio dimensionale per la loro individuazione (per superare i gravi limiti soggettivi nella individuazione dei soggetti tenuti, visto che la NIS 1 lasciava liberi gli Stati Membri di individuare criteri nazionali, determinandosi una frammentazione delle regole);
- la razionalizzazione dei requisiti minimi di sicurezza e delle procedure di notifica obbligatoria;
- l'adozione di un approccio "multirischio";
- la regolamentazione della divulgazione coordinata delle vulnerabilità (CVD) e le specifiche funzioni di coordinamento attribuite agli CSIRT nazionali;
- l'implementazione delle misure di cooperazione, al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala.

PROPRIETA' INDUSTRIALE

5 Giugno 2024 – Tribunale UE: la McDonald's perde il marchio dell'Unione europea "*Big Mac*" per i prodotti a base di pollame.

Il Tribunale UE ha deciso che per alcuni prodotti e servizi la McDonald's non ha dimostrato un uso effettivo per un periodo ininterrotto di cinque anni nell'Unione. Il caso ha visto contrapposte la Supermac's e la McDonald's, rispettivamente, una catena di ristorazione rapida irlandese e la nota azienda americana in merito all'utilizzo del marchio dell'Unione europea "*Big Mac"*. Tale marchio era stato registrato a favore della McDonald's nel 1996. Nel 2017 la Supermac's ha presentato una domanda di decadenza di tale marchio rispetto a taluni prodotti e servizi. Essa riteneva infatti che il marchio non fosse stato oggetto di un uso effettivo per detti prodotti e servizi nell'Unione per un periodo ininterrotto di cinque anni.

L'Ufficio dell'Unione europea per la proprietà intellettuale (EUIPO) ha parzialmente accolto tale domanda. Esso ha tuttavia confermato la tutela conferita dal marchio contestato alla McDonald's, in particolare, per gli alimenti a base di carne e di pollame e i panini con carne e con pollo, nonché per servizi forniti o connessi alla gestione di ristoranti e di altri locali o infrastrutture di ristorazione per il consumo e il «drive-in» e per la preparazione di piatti da asporto.

Con la sua sentenza, il Tribunale annulla e riforma parzialmente la decisione dell'EUIPO, limitando così ulteriormente la tutela conferita dal marchio contestato alla McDonald's. Infatti, il Tribunale dichiara che la McDonald's non ha dimostrato che il marchio contestato sia stato oggetto di un uso effettivo per quanto riguarda i prodotti «panini con pollo», i prodotti «alimenti a base di pollame» e i servizi «forniti o connessi alla gestione di ristoranti e di altri locali o infrastrutture di ristorazione per il consumo e il "drive-in", preparazione di piatti da asporto».

Le prove prodotte dalla McDonald's non forniscono alcuna indicazione sull'entità dell'uso del marchio per tali prodotti e segnatamente per quanto concerne il volume delle vendite, la durata del periodo in cui gli atti di uso sono stati compiuti e la loro frequenza. Pertanto, le prove prese in considerazione dall'EUIPO non consentono di dimostrare l'esistenza di un uso effettivo del marchio contestato per detti prodotti. In più, gli elementi di prova prodotti dalla McDonald's non consentono di dimostrare che il marchio contestato sia stato utilizzato per i «servizi forniti o connessi alla gestione di ristoranti e di altri locali o infrastrutture di ristorazione per il consumo e il "drive-in"; preparazione di piatti da asporto»