FIVERS

Aggiornamento
Data protection, AI, IT e IP

n. 11 / 2024

DATA PROTECTION

26 Settembre 2024 – Suprema Corte di Cassazione: non viola la privacy produrre un file audio in giudizio per la tutela di un diritto fondamentale.

---

27 Settembre 2024 – Corte di Giustizia UE: l'autorità di controllo non è tenuta ad adottare una misura correttiva in tutti i casi di violazione e, in particolare, a infliggere una sanzione pecuniaria.

INTELLIGENZA ARTIFICIALE.

25 Settembre 2024 – Commissione UE: oltre cento aziende sottoscrivono l'AI Pact della UE per anticipare l'applicazione di talune prescrizioni del Regolamento UE sull'Intelligenza Artificiale.

---

25 Settembre 2024 – Commissione UE: in dirittura di arrivo i lavori sul codice di buone pratiche per l'intelligenza artificiale di uso generale.

---

24 settembre 2024 - Europol ha pubblicato un rapporto sui benefici e le sfide dell'intelligenza artificiale (AI) per le forze dell'ordine.

MDERCATI DIGITALI

25 Settembre 2024 – Il Gruppo di esperti informatici del G7 raccomanda azioni per combattere i rischi del settore finanziario derivanti dall'informatica quantistica.

INFORMATION TECHNOLOGY

25 Settembre 2024 – Pubblicato il D.lgs. 4 settembre 2024, n. 134 recante «Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici".

DATA PROTECTION

26 Settembre 2024 – Suprema Corte di Cassazione: non viola la privacy produrre un file audio in giudizio per la tutela di un diritto fondamentale.

Difendersi in giudizio, specie ove la controversia attenga a diritti della persona strettamente connessi alla dignità umana - e quindi i diritti dei lavoratori, secondo quanto dispone l'art. 36 Cost. - è un diritto fondamentale e, nella relazione tra il datore di lavoro e i dipendenti, si creano legittime aspettative e, tra queste, quella della reciproca lealtà e del rispetto dei diritti del dipendente; gli artt. 17 e 21 del GDPR rendono palese che, nel bilanciamento degli interessi in gioco, il diritto a difendersi in giudizio può essere ritenuto prevalente sui diritti dell'interessato al trattamento dei dati personali; in particolare, l'art. 17 comma 3 lettera e) del GDPR dispone che i paragrafi 1 e 2 (diritto alla cancellazione) non si applicano nella misura in cui il trattamento sia necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria e l'art 21 (diritto di opposizione) consente al titolare del trattamento di dimostrare "*l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria*".

In questo modo si è espressa la Cassazione civile con l'ordinanza n. 24797/2024 con la quale ha riconosciuto il diritto di alcuni lavoratori a produrre in giudizio un file audio contenente la registrazione di una conversazione (tra l'altro risalente ad anni prima) con i dirigenti e rappresentanti legali dell'impresa che avevano fatto ricorso al Garante (respinto) per violazione del principio di liceità e correttezza nel trattamento. Il Tribunale di Venezia aveva annullato il provvedimento del Garante privacy, mentre la Cassazione ha disposto l'annullamento con rinvio sulla base delle considerazioni sopra illustrate.

---

27 Settembre 2024 – Corte di Giustizia UE: l'autorità di controllo non è tenuta ad adottare una misura correttiva in tutti i casi di violazione e, in particolare, a infliggere una sanzione pecuniaria.

In Germania, una Cassa di risparmio ha constatato che una delle sue dipendenti aveva consultato più volte, senza esservi autorizzata, i dati personali di un cliente. La Cassa di risparmio non ne ha informato quest'ultimo in quanto il suo responsabile della protezione dei dati aveva ritenuto che non vi fosse per lui un rischio elevato. Infatti, la dipendente aveva confermato per iscritto di non aver né copiato né conservato i dati, di non averli trasmessi a terzi e che non lo avrebbe fatto in futuro. Inoltre, la Cassa di risparmio aveva adottato provvedimenti disciplinari nei suoi confronti. La Cassa di risparmio ha comunque notificato tale violazione al commissario per la protezione dei dati del Land.

Dopo essere venuto incidentalmente a conoscenza di tale fatto, il cliente ha presentato un reclamo dinanzi a detto commissario per la protezione dei dati. Dopo aver sentito la Cassa di risparmio, il commissario per la protezione dei dati ha informato il cliente che non riteneva necessario adottare misure correttive nei confronti della Cassa di risparmio.

Il cliente ha quindi proposto un ricorso dinanzi a un giudice tedesco, chiedendogli di ingiungere al commissario per la protezione dei dati di intervenire nei confronti della Cassa di risparmio e, in particolare, di infliggerle una sanzione pecuniaria.

Il giudice tedesco ha chiesto alla Corte di interpretare il regolamento generale sulla protezione dei dati (RGPD) al riguardo.

La Corte risponde che, in caso di accertamento di una violazione di dati personali, l'autorità di controllo non è tenuta ad adottare una misura correttiva, in particolare l'irrogazione di una sanzione amministrativa, qualora ciò non sia necessario al fine di porre rimedio alla carenza rilevata e garantire il pieno rispetto del

RGPD. Ciò potrebbe verificarsi, in particolare, qualora il titolare del trattamento, non appena ne sia venuto a conoscenza, abbia adottato le misure necessarie affinché detta violazione cessi e non si ripeta.

Il RGPD lascia all'autorità di controllo un margine di discrezionalità quanto al modo in cui essa deve porre rimedio all'inadeguatezza constatata. Tale margine è limitato dalla necessità di garantire un livello coerente ed elevato di protezione dei dati personali mediante un'applicazione rigorosa del RGPD.

Spetta al giudice tedesco verificare se il commissario per la protezione dei dati abbia rispettato tali limiti.

INTELLIGENZA ARTIFICIALE.

25 Settembre 2024 – Commissione UE: oltre cento aziende sottoscrivono l'AI Pact della UE per anticipare l'applicazione di talune prescrizioni del Regolamento UE sull'Intelligenza Artificiale.

La Commissione UE ha annunciato che oltre un centinaio di imprese hanno sottoscritto il Patto dell'UE sull'intelligenza artificiale (IA) aderendo fin da ora ai suoi impegni volontari. I firmatari includono multinazionali e piccole e medie imprese (PMI) europee di diversi settori, tra cui IT, telecomunicazioni, sanità, banche, automotive e aeronautica. L'AI Pact sostiene gli impegni volontari dell'industria di iniziare ad applicare i principi del Regolamento 2024/1689 prima della sua entrata in vigore e rafforza l'impegno tra l'Ufficio dell'UE per l'IA e tutti i portatori di interessi, tra cui l'industria, la società civile e il mondo accademico.

Gli impegni volontari del Patto dell'UE per l'IA richiedono alle imprese partecipanti a impegnarsi in almeno tre azioni fondamentali:

1. **Strategia di governance dell'IA** per promuovere l'adozione dell'IA nell'organizzazione e lavorare per la futura conformità con l'AI Act.
2. **Mappatura dei sistemi di IA ad alto rischio**: identificazione dei sistemi di IA che possono essere classificati come ad alto rischio ai sensi della legge sull'IA
3. **Promuovere l'alfabetizzazione e la consapevolezza dell'IA tra il personale,** garantendo uno sviluppo etico e responsabile dell'IA.

Oltre a questi impegni fondamentali, più della metà dei firmatari si è impegnata a sottoscrivere ulteriori impegni, tra cui garantire la supervisione umana, mitigare i rischi ed etichettare in modo trasparente alcuni tipi di contenuti generati dall'intelligenza artificiale, come i deepfake.

Oltre agli sforzi volti ad aiutare le imprese ad attuare la legge sull'IA in previsione della scadenza legale, la Commissione Europea sta adottando misure per promuovere l'innovazione dell'UE nel settore dell'IA. L'iniziativa *AI Factories* del 10 settembre 2024 fornirà alle start-up e all'industria uno sportello unico per innovare e sviluppare l'intelligenza artificiale, compresi i dati, il talento e la potenza di calcolo. Le *AI Factories* promuoveranno inoltre lo sviluppo e la convalida di applicazioni industriali e scientifiche dell'intelligenza artificiale in settori europei chiave come la sanità, l'energia, l'*automotive* e i trasporti, la difesa e l'aerospaziale, la robotica e l'industria manifatturiera, le tecnologie pulite e l'*agritech.*

Le *AI Factories* sono uno dei punti salienti del pacchetto di innovazione dell'IA della Commissione UE presentato nel gennaio 2024, insieme alle misure di sostegno al capitale di rischio e al capitale proprio, alla realizzazione di spazi comuni europei di dati, all'iniziativa "GenAI4EU" e alla grande grande sfida sull'IA che offre alle start-up sostegno finanziario e accesso ai supercomputer dell'UE, tra le altre misure.

La Commissione istituirà inoltre un *Consiglio europeo per la ricerca sull'IA* per sfruttare il potenziale dei dati e la strategia per l'applicazione dell'IA per promuovere nuovi usi industriali dell'IA.

25 Settembre 2024 – Commissione UE: in dirittura di arrivo i lavori sul codice di buone pratiche per l'intelligenza artificiale di uso generale.

La Commissione UE ha ricevuto quasi 430 osservazioni in risposta alla sua consultazione multilaterale sull'imminente *Codice di buone pratiche per l'intelligenza artificiale di uso generale (GPAI),* come previsto dal Regolamento 2024/1689.

Le osservazioni ricevute saranno utili per il lavoro della Commissione volto a mettere a punto il codice di buone pratiche entro aprile 2025. Le disposizioni della legge sull'IA sull'Intelligenza Artificiale per scopi generali - GPAI entreranno in vigore 12 mesi dopo l'entrata in vigore della legge, il 1° agosto 2025.

Le principali aree di interesse del Codice includono la trasparenza, le norme relative al diritto d'autore, la valutazione e la mitigazione dei rischi e la relativa governance interna. Inoltre, i contributi ricevuti contribuiranno a guidare il lavoro dell'Ufficio per l'IA, che supervisionerà l'attuazione e l'applicazione delle norme dell'AI Act sulla GPAI. Quest contributi saranno inoltre utilizzati dall'Ufficio per l'IA per sviluppare un *template* e linee guida per riassumere le regole in merito ai dati di addestramento utilizzati nei modelli GPAI.

La consultazione fa parte degli sforzi più ampi della Commissione UE per promuovere lo sviluppo responsabile dell'intelligenza artificiale. I contributi sono stati presentati da una vasta gamma di portatori di interessi, tra cui fornitori di GPAI, fornitori a valle, organizzazioni industriali, mondo accademico, società civile, titolari di diritti e altri gruppi pertinenti, che offrono prospettive diverse su come garantire un'IA affidabile e responsabile all'interno dell'UE.

La consultazione si è aggiunta a un invito a manifestare interesse a partecipare all'elaborazione del primo codice di buone pratiche per l'IA per uso generale, che ha attirato quasi 1000 organizzazioni e individui in tutto il mondo. La sessione plenaria introduttiva si è tenuta lo scorso 30 settembre 2024 on line.

---

24 settembre 2024 - Europol ha pubblicato un rapporto sui benefici e le sfide dell'intelligenza artificiale (AI) per le forze dell'ordine.

Un nuovo rapporto di Europol intitolato "*AI e attività di pubblica sicurezza: vantaggi e sfide dell'intelligenza artificiale per le forze dell'ordine*" fa luce su come le tecnologie che utilizzano l'intelligenza artificiale, in particolare il riconoscimento facciale, vengono integrate nelle forze dell'ordine, mentre crescono le preoccupazioni per la privacy e i diritti civili.

La valutazione di Europol evidenzia i potenziali benefici che l'IA può apportare alle forze dell'ordine, attraverso l'uso della polizia predittiva e l'analisi di grandi insiemi di dati in tempo reale.

Secondo il rapporto, l'IA sta trasformando il modo di operare delle forze di polizia. Gli strumenti di IA, tra cui il riconoscimento facciale, vengono utilizzati per semplificare la prevenzione dei crimini, accelerare le indagini e contribuire all'identificazione delle reti criminali, oltre che per localizzare persone e bambini scomparsi, confrontando le immagini di individui non identificati con i database delle persone scomparse. Tuttavia, l'adozione dell'IA ha sollevato questioni etiche e legali, in particolare per quanto riguarda i pregiudizi.

Secondo il rapporto Europol, le forze dell'ordine si affidano sempre più a tecnologie basate sull'IA, come l'analisi dei dati, il riconoscimento dei modelli e i sistemi decisionali. Questi sistemi aiutano le forze dell'ordine a migliorare l'individuazione e la prevenzione dei reati. La capacità dell'IA di analizzare i dati provenienti da varie fonti, come i filmati delle telecamere a circuito chiuso e i social media, può fornire alla polizia indizi cruciali, sottolinea il rapporto.

Tuttavia, Europol sottolinea la necessità di bilanciare la tecnologia con la responsabilità e la trasparenza. Con la crescente diffusione dei sistemi di intelligenza artificiale, sono aumentate le preoccupazioni per i pregiudizi, l'uso improprio dei dati personali e la violazione dei diritti individuali. Europol sottolinea l'importanza di quadri etici e di una supervisione normativa per evitare che le attività di polizia guidate dall'IA violino le libertà civili.

MERCATI DIGITALI

25 Settembre 2024 – Il Gruppo di esperti informatici del G7 raccomanda azioni per combattere i rischi del settore finanziario derivanti dall'informatica quantistica.

Il Cyber Expert Group (CEG) del G7 ha rilasciato una dichiarazione pubblica che evidenzia i potenziali rischi per la sicurezza informatica associati agli sviluppi dell'informatica quantistica e raccomanda alle autorità e alle istituzioni finanziarie di adottare misure per affrontare tali rischi.

Il CEG del G7 è composto da rappresentanti delle autorità finanziarie di tutti i Paesi del G7 e dell'Unione europea. È stato fondato nel 2015 per fungere da gruppo di lavoro che coordina la politica e la strategia di cybersicurezza nelle giurisdizioni dei Paesi membri.

Gli attuali scenari tecnologici vedono la costruzione di computer quantistici in grado di risolvere in tempi ragionevoli problemi di calcolo attualmente ritenuti impossibili per i computer tradizionali. Se da un lato tali potenti computer possono offrire vantaggi significativi al sistema finanziario, dall'altro comportano rischi unici per la sicurezza informatica. Uno dei più significativi è che gli attori delle minacce informatiche potrebbero utilizzare i computer quantistici per scardinare le tecniche crittografiche che proteggono le comunicazioni e i sistemi informatici, esponendo potenzialmente i dati delle entità finanziarie, comprese le informazioni sui clienti.

Sebbene la tempistica esatta per lo sviluppo di computer quantistici con queste capacità sia incerta, esiste la possibilità concreta che tali capacità possano emergere entro un decennio. I computer quantistici non metterebbero a rischio solo i dati futuri, ma anche tutti i dati trasmessi in precedenza ed eventualmente carpiti, con l'intento di decrittarli poi con i computer quantistici. A causa dei tempi potenzialmente lunghi necessari per l'implementazione di tecnologie *quantum-resilienti*, è appunto questo il momento di iniziare a pianificare le opportune strategie difensive: proprio in questa ottica, ad esempio, l'americano *National Institute of Standards and Technology (*NIST) ha appena pubblicato una prima serie di standard di crittografia quantistica e in futuro è previsto il rilascio di ulteriori standard, sempre da parte del NIST.

Con la disponibilità degli standard del NIST, alcune entità finanziarie potrebbero essere in grado di iniziare ad apportare le modifiche necessarie per implementare le tecnologie *quantum-resilienti* all'interno dei loro sistemi. Il CEG del G7 incoraggia le autorità e le istituzioni finanziarie a iniziare ad adottare le seguenti misure per costruire la resilienza contro i rischi dell'informatica quantistica:

1. Sviluppare una migliore comprensione del problema, dei rischi connessi e delle strategie per mitigarli.

2. Valutare i rischi legati all'informatica quantistica nelle loro aree di responsabilità.

3. Sviluppare un piano per mitigare i rischi legati all'informatica quantistica.

La dichiarazione del CEG fornisce ulteriori dettagli sui rischi dell'informatica quantistica e sulle azioni specifiche che le entità finanziarie possono iniziare a intraprendere per costruire la resilienza quantistica all'interno del sistema finanziario.

INFORMATION TECHNOLOGY

25 Settembre 2024 – Pubblicato il D.lgs. 4 settembre 2024, n. 134 recante «Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici".

Con la Direttiva (UE) 2022/2557 (*Direttiva CER*) si interviene per:

- realizzare un adeguato livello di armonizzazione nell'individuazione dei settori, dei sottosettori e delle categorie dei soggetti qualificabili come critici;
- rafforzare la loro resilienza, intesa come capacità di prevenire, proteggere, rispondere, resistere, mitigare, assorbire, adattarsi e ripristinare le proprie capacità operative a seguito di incidenti che possono perturbare la fornitura di servizi essenziali.

Soggetto critico: un soggetto pubblico o privato individuato nell'ambito delle categorie di soggetti che operano nei settori e sottosettori di cui all'allegato A del presente provvedimento. I soggetti critici sono individuati almeno nei seguenti settori:

- energia;
- trasporti;
- bancario;
- infrastrutture dei mercati finanziari;
- salute;
- acqua potabile;
- acque reflue;
- Infrastrutture digitali;
- spazio;
- produzione, trasformazione e distribuzione di alimenti;
- enti della pubblica amministrazione.

Nello specifico, il D.lgs. n. 134/2024 stabilisce:

- misure volte a garantire che i **servizi essenziali** per il mantenimento di funzioni vitali della società, di attività economiche, della salute e della sicurezza pubbliche o dell'ambiente siano forniti senza impedimenti nonché criteri per l'individuazione dei soggetti critici;
- obblighi per i soggetti critici, volti a rafforzarne la resilienza, fino al raggiungimento di un livello elevato, e a rafforzarne la capacità di fornire i servizi essenziali, nel mercato interno, al fine di migliorarne il funzionamento;
- misure per il sostegno nell'adempimento degli obblighi imposti ai soggetti critici;
- disposizioni riguardanti la vigilanza e l'irrogazione di sanzioni nei confronti dei soggetti critici;
- disposizioni riguardanti l'individuazione dei soggetti critici di particolare rilevanza europea e le missioni di consulenza della Commissione europea finalizzate a valutare le misure predisposte da tali soggetti per adempiere ai propri obblighi;
- disposizioni per la predisposizione della *strategia nazionale per la resilienza* dei soggetti critici;
- la disciplina della valutazione del rischio da parte dello Stato e della valutazione del rischio da parte dei soggetti critici;
- l'istituzione del Comitato interministeriale per la resilienza, nonché l'individuazione delle autorità settoriali competenti e del punto di contatto unico;
- le modalità di cooperazione con gli altri Stati membri e con la Commissione europea, inclusa la partecipazione nazionale al gruppo per la resilienza dei soggetti critici.

Misure di resilienza dei soggetti critici.

I soggetti critici dovranno adottare e applicare misure tecniche, di sicurezza e di organizzazione, adeguate e proporzionate, per garantire la propria resilienza, sulla base delle informazioni pertinenti fornite in merito alla valutazione del rischio dello Stato, messe a disposizione dal PCU.
Il punto di contatto unico (PCU), istituito nell'ambito della Presidenza del Consiglio dei Ministri, al esercita le funzioni di:

- assicurare il collegamento con la Commissione europea e la cooperazione con i Paesi terzi;
- coordinare le attività di sostegno ai soggetti critici nel rafforzamento della loro resilienza;
- ricevere, da parte dei soggetti critici, contestualmente alle autorità competenti, le notifiche degli incidenti che perturbano o possono perturbare in modo significativo la fornitura di servizi essenziali;
- promuovere le attività di ricerca e formazione in materia di resilienza delle infrastrutture critiche;
- coordinare l'attività delle autorità competenti.

Nello specifico, è prevista:

- una valutazione del rischio, con l'adozione di misure tecniche, di sicurezza e organizzative, adeguate e proporzionate per garantire la resilienza e ripristinare le capacità operative in caso di incidenti;
- il contrasto e il resistere alle conseguenze degli incidenti, nonché la loro mitigazione, anche considerando procedure e protocolli di gestione dei rischi e delle crisi, nonché pratiche di allerta;
- la notifica senza ritardo all'autorità competente degli incidenti che perturbano o possono perturbare in modo significativo la fornitura di servizi essenziali;
- l'adozione di una strategia.