FIVERS

Aggiornamento
Data protection, AI, IT e IP

n. 3 / 2025

DATA PROTECTION.

5 Febbraio 2024 – Corte Suprema di Cassazione: l'ordinanza 807/2025 precisa che i controlli difensivi sulla e-mail del lavoratore non possono essere retroattivi rispetto all'insorgenza del sospetto di illecito.

1° Febbraio 2025 – L'Autorità Garante per la protezione dei dati personali francese (CNIL) pubblica una guida su come effettuare la Data Transfer Impact Assessment (DTIA).

---

31 Gennaio 2025 – L'Autorità Garante per la protezione dei dati personali francese (CNIL) ha posto in consultazione pubblica uno schema europeo di certificazione del Responsabile esterno del trattamento dei dati personali.

INTELLIGENZA ARTIFICIALE.

4 febbraio 2025 – Commessione UE: pubblicate le Linee Guida sulle pratiche di Intelligenza Artificiale vietate ai sensi del Regolamento 2024/1689 (AI Act).

---

2 Febbraio 2024 – Regolamento UE 2024/1689 sull'Intelligenza Artificiale: applicabili i primi 5 articoli.

---

23 Gennaio 2024 – Comitato europeo per la protezione dei dati personali: diffusi due rapporti su (1) governance dei dati contro la discriminazione algoritmica e (2) effettività dell'esercizio dei diritti data protection nel contesto AI.

MERCATI DIGITALI

2 Febbraio 2025 – Schema di decreto legislativo di coordinamento del Regolamento 2022/2554 sulla resilienza operativa digitale (DORA) all'ordinamento nazionale.

INFORMATION TECHNOLOGY

28 Gennaio 2025 – Corte di Cassazione: anche se il destinatario di una PEC afferma di non aver ricevuto la notifica, la stessa si perfeziona con la ricevuta di avvenuta consegna.

---

24 Gennaio 2025 – Corte Costituzionale: incostituzionali le norme del Codice dell'Amministrazione Digitale (CAD) che hanno l'effetto di impedire ai disabili l'uso della firma digitale per sottoscrivere le liste elettorali.

DATA PROTECTION

5 Febbraio 2024 – Corte Suprema di Cassazione: l'ordinanza 807/2025 precisa che i controlli difensivi sulla e-mail del lavoratore non possono essere retroattivi rispetto all'insorgenza del sospetto di illecito.

La Corte di Cassazione, con l'ordinanza n. 807/2025, ha fornito indicazioni rilevanti riguardo ai controlli difensivi e ai limiti di tali controlli che i datori di lavoro possono effettuare sulle e-mail aziendali dei propri dipendenti nel caso sorga un sospetto di illecito.
La decisione stabilisce che tali verifiche non possono essere retroattive, ossia non possono riguardare comunicazioni antecedenti al sorgere del fondato sospetto di illecito che abilita il controllo difensivo.

La possibilità per i datori di lavoro di monitorare le comunicazioni via e-mail dei lavoratori a scopo di controllo difensivo ha generato numerose discussioni giuridiche, portando la Cassazione a definire con maggiore precisione i limiti entro cui tali controlli possono avvenire.

Con la sua recente ordinanza, la Suprema Corte ha chiarito che i controlli difensivi da parte dell'azienda sono legittimi solo se condotti su dati raccolti dopo l'emergere di sospetti concreti.

Uno degli aspetti fondamentali sanciti dalla Cassazione è l'impossibilità di esaminare le email inviate o ricevute prima che sorga il dubbio su una possibile irregolarità. Questa limitazione è necessaria per garantire un equilibrio tra la protezione degli interessi aziendali e il diritto alla privacy dei lavoratori, entrambi tutelati dalle normative vigenti.

1° Febbraio 2025 – L'Autorità Garante per la protezione dei dati personali francese (CNIL) pubblica una guida su come effettuare la Data Transfer Impact Assessment (DTIA).

L'autorità francese per la protezione dei dati, CNIL, ha pubblicato una guida alla valutazione dell'impatto sul trasferimento dei dati (DTIA) per aiutare le organizzazioni a trasferire dati personali al di fuori dello Spazio economico europeo (SEE) in conformità con il GDPR.

La guida delinea il processo per l'esecuzione di una DTIA quando si utilizzano clausole contrattuali standard (SCC) o norme vincolanti d'impresa (BCR) e dettagli quando una DTIA non è richiesta, ad esempio per i paesi con una decisione di adeguatezza o esenzioni ai sensi dell'articolo 49.

Fornisce una *roadmap* in cinque fasi per l'esecuzione di una DTIA e raccomanda sei misure per garantire un trasferimento efficace dei dati, tra cui la valutazione delle leggi dei paesi terzi, l'identificazione dei rischi e l'attuazione di misure aggiuntive.

---

31 Gennaio 2025 – L'Autorità Garante per la protezione dei dati personali francese (CNIL) ha posto in consultazione pubblica uno schema europeo di certificazione del Responsabile esterno del trattamento dei dati personali.

L'autorità francese per la protezione dei dati, CNIL, ha avviato una consultazione per un sistema di certificazione dei responsabili del trattamento dei dati ai sensi del GDPR, aperto alle organizzazioni europee che trattano dati personali per conto di un titolare del trattamento.

In particolare, la CNIL ha evidenziato che tutte le organizzazioni con sede in Europa che elaborano dati personali per conto di un titolare del trattamento dei dati potranno richiedere la certificazione. Le piccole e medie imprese sono incoraggiate a presentare domanda. Gli obblighi dei responsabili del trattamento si applicano a tutte le organizzazioni che elaborano i dati per conto di un titolare del trattamento dei dati e possono includere: fornitori di servizi IT; software house ; società di sicurezza informatica; società di servizi digitali che hanno accesso ai dati; società di marketing o comunicazione.

La certificazione è concepita per essere generalista, copre un'ampia gamma di attività di trattamento dei

dati e comprende 90 punti di controllo in cinque parti, dalla contrattazione ai piani d'azione durante il periodo di certificazione di tre anni. La consultazione pubblica terminerà il 28 febbraio 2025.

INTELLIGENZA ARTIFICIALE.

4 febbraio 2025 – Commessione UE: approvate le Linee Guida sulle pratiche di Intelligenza Artificiale vietate ai sensi del Regolamento 2024/1689 (AI Act).

In concomitanza con la diretta applicabilità – a far data dal 2 febbraio 2025 – dell'articolo 5 del Regolamento 2024/1689 sull'IA, che reca il divieto delle cosiddette "*pratiche di intelligenza artificiale vietate*" la Commissione UE ha approvato (anche se non ancora formalmente adottato) la Comunicazione recante le Linee Guida sulle pratiche di IA vietate ai sensi del Regolamento UE 2024/1689.

Le linee guida affrontano specificamente – con indicazioni operative e interpretative (non vincolanti) sui divieti – pratiche come la manipolazione dannosa, il punteggio sociale e l'identificazione biometrica remota in tempo reale, tra le altre. Forniscono inoltre chiarimenti legali ed esempi pratici utili a comprendere e rispettare i requisiti dell'AI Act.

Molto concreta e utile l'impostazione degli orientamenti: per ogni pratica di IA vietata la Commissione fornisce una analisi su logica normativa, obiettivi del divieto, principali caratteristiche concettuali e interpretative, tipologia di comportamenti che rientrano nel divieto, comportamenti legali o al di fuori del divieto, interconnessione con altre normative della UE (es: il GDPR), casi di esclusione, esempi pratici.

---

2 Febbraio 2024 – Regolamento UE 2024/1689 sull'Intelligenza Artificiale: applicabili i primi 5 articoli.

A partire dal 2 febbraio 2025 comincia ad essere applicabile il Regolamento UE 2024/1689 sull'Intelligenza Artificiale. Il cosiddetto AI Act è entrato il vigore il 1° agosto 2024, ma sarà applicabile a scadenze differite, tra 6 e 36 mesi dalla data di entrata in vigore. Dal 2 febbraio 2025 sono pienamente applicabili i Capi I e II e ai primi 5 articoli dell'AI Act. Dal punto di vista pratico, ad esempio, è possibile fare uso (nei contratti di fornitura) delle 68 definizioni tecniche di cui all'articolo 3 (a partire dalla definizione di "*sistema di intelligenza artificiale*" e di "*modello di intelligenza artificiale*"), mentre diviene obbligatoria per fornitori, imprese e utilizzatori la "*alfabetizzazione in materia di IA*" cioè l'obbligo (anche formativo) di avere personale sufficientemente formato e con competenze di base nell'utilizzo dell'IA. È infine applicabile il divieto di talune pratiche di intelligenza artificiale, alcune delle quali riguardano l'uso dell'IA nei luoghi di lavoro.

---

24 Gennaio 2024 – Comitato europeo per la protezione dei dati personali: diffusi due rapporti su (1) governance dei dati contro la discriminazione algoritmica e (2) effettività dell'esercizio dei diritti data protection nel contesto AI.

Il Comitato europeo per la protezione dei dati (EDPB) ha pubblicato i due rapporti (1) "*AI-Complex Algorithms and effective Data Protection Supervision - Bias evaluation*" e (2) "*AI-Complex Algorithms and effective Data Protection Supervision - Effective implementation of data subjects' rights*".

Il rapporto sulla valutazione della discriminazione algoritmica (blas) identifica varie fonti di bias nell'intelligenza artificiale, a partire dai dati incompleti o inesatti, e propone misure di mitigazione sia nella fase di pre-trattamento che nella successiva fase di post-elaborazione nel *machine learning*. Tale rapporto riconosce inoltre gli attuali limiti degli strumenti per rilevare e mitigare i pregiudizi nei sistemi di intelligenza artificiale generativa.

Nel secondo rapporto sulla implementazione dei diritti degli interessati nel contesto AI l'analisi esamina le sfide legate all'attuazione dei diritti degli interessati nell'IA, proponendo metodi per la cancellazione e l'*unlearning* dei dati o la *privacy differenziale* per limitare l'influenza dei singoli punti di dati. L'*unlearning* o *disapprendimento* si riferisce al processo di rimuovere conoscenze o informazioni apprese da un modello

di apprendimento automatico o da un sistema AI. Vi sono sostanzialmente due approcci: **(1)** *l'unlearning indipendente dal modello*, che non dipende dall'architettura o dal funzionamento specifico del modello ed è un metodo generico applicabile a qualsiasi sistema, indipendentemente dal tipo di modello sottostante; e **(2)** *l'unlearning specifico dell'applicazione*, che invece si basa sull'adattamento del metodo di unlearning al modello o al caso specifico, sfruttando la conoscenza dell'architettura e del funzionamento del sistema.

La *privacy differenziale (Differential Privacy, DP*) è un quadro matematico utilizzato per proteggere la privacy delle persone fisiche in un dataset, limitando l'influenza dei singoli punti di dati sul risultato di un'analisi o di un modello. In sostanza, un meccanismo soddisfa la privacy differenziale se l'aggiunta o la rimozione di un singolo dato nel dataset cambia in modo trascurabile il risultato dell'algoritmo. Ciò garantisce che i dati personali di un individuo non possano essere identificati o ricostruiti, anche quando il modello o il risultato sono pubblicati.

MERCATI DIGITALI

2 Febbraio 2025 – Schema di decreto legislativo di coordinamento del Regolamento 2022/2554 sulla resilienza operativa digitale (DORA) all'ordinamento nazionale.

Lo schema di decreto attuativo coordina con l'ordinamento nazionale le disposizioni del Regolamento (UE) 2022/2554 (DORA) e si articola in sei capi, definendo, tra l'altro, le Autorità competenti a livello nazionale e il ruolo del *Computer Security Incident Response Team* (CSIRT) Italia.

Ai sensi dell'articolo 46 del Regolamento DORA, le competenze in materia di vigilanza sono ripartite tra diverse Autorità, ciascuna delle quali esercita le proprie funzioni secondo specifiche attribuzioni. In particolare:

- Banca d'Italia: esercita poteri di vigilanza sugli intermediari finanziari, su Bancoposta e su Cassa Depositi e Prestiti S.p.A., garantendo il rispetto degli obblighi previsti dal Regolamento DORA;

- Consob: partecipa in qualità di osservatore al forum di sorveglianza;

- IVASS e COVIP: intervengono in funzione di osservatori in relazione alle materie di rispettiva competenza.

In applicazione delle disposizioni del Regolamento DORA, dei relativi atti delegati, delle norme tecniche di regolamentazione e di attuazione, nonché delle disposizioni attuative dello schema di decreto, le Autorità competenti dispongono di specifici poteri di vigilanza. Tali poteri includono la facoltà di adottare misure di intervento nei confronti delle entità finanziarie soggette a vigilanza; di Cassa Depositi e Prestiti S.p.A.; degli intermediari finanziari e di Bancoposta; dei fornitori terzi di servizi ICT (TIC) che supportano *funzioni essenziali o importanti* per il settore finanziario.

I poteri di vigilanza, sanciti dagli articoli 50, paragrafo 2, e 42, paragrafo 6, del Regolamento DORA, si estendono a quelli già previsti dalla normativa di settore e dallo schema di decreto attuativo. In concreto, le Autorità possono effettuare accessi ispettivi e verifiche presso i fornitori terzi di servizi TIC; convocare amministratori, membri del collegio sindacale e personale delle entità vigilate; richiedere informazioni, documentazione e chiarimenti in merito alla gestione del rischio ICT.
Tali poteri si aggiungono a quelli già attribuiti da discipline settoriali, tra cui il Testo Unico Bancario (TUB), il Testo Unico della Finanza (TUF) e il Codice delle Assicurazioni Private (CAP). Rientrano, inoltre, tra gli strumenti di intervento le disposizioni contenute negli articoli 51, 53-bis, 54 e 108 del TUB, nonché altre norme correlate.

Uno degli aspetti di maggior rilievo dello schema di decreto è rappresentato dal regime sanzionatorio delineato dall'articolo 10. Il sistema prevede un'articolazione su più livelli di responsabilità, in funzione della gravità della violazione accertata.

Le sanzioni pecuniarie possono raggiungere il 10% del fatturato annuo dell'entità finanziaria responsabile, con differenziazioni in base alla tipologia di soggetto vigilato:

- Banche, intermediari finanziari e fornitori di servizi TIC: sanzioni pecuniarie comprese tra un minimo di 30.000 euro e un massimo pari al 10% del fatturato.
- Istituti di pagamento e istituti di moneta elettronica: sanzioni fino a 5 milioni di euro o al 10% del fatturato annuo, a seconda dell'importo più elevato.
- Amministratori, dirigenti e personale con funzioni specifiche: per le infrazioni più gravi, possono essere comminate sanzioni fino a 5 milioni di euro.

Accanto alle sanzioni pecuniarie, il decreto prevede misure di carattere accessorio, applicabili nei casi di violazioni particolarmente gravi. Tra queste rientrano:

- interdizione temporanea dagli incarichi di amministrazione, direzione o controllo per i soggetti responsabili delle infrazioni;
- limitazioni operative per le entità vigilate, ove necessario per la tutela della stabilità del sistema finanziario.

L'apparato sanzionatorio introdotto dallo schema di decreto si inserisce in un quadro normativo più ampio, volto a garantire l'effettiva attuazione delle disposizioni del Regolamento DORA e a rafforzare la resilienza digitale del settore finanziario.

INFORMATION TECHNOLOGY

28 Gennaio 2025 – Corte di Cassazione: anche se il destinatario di una PEC afferma di non aver ricevuto la notifica, la stessa si perfeziona con la ricevuta di avvenuta consegna.

La Corte di appello aveva ha dichiarato inammissibile, in quanto tardivamente proposto, l'appello proposto avverso la sentenza di primo grado che aveva rigettato una domanda risarcitoria. A fondamento della sua decisione, la Corte aveva ritenuto idonea a far decorrere il termine breve per impugnare ex art. 326 c.p.c. la notifica della sentenza di primo grado effettuata a mezzo PEC al procuratore costituito dall'attore.

La controversia giunge in Cassazione dove il ricorrente censura la sentenza impugnata per non aver la Corte d'Appello tenuto conto della normativa sulla certezza delle notificazioni alle parti, sostenendo in tal senso che le risposte ricevute alle richieste inviate dal difensore dell'appellante al gestore di posta elettronica certificata provano che egli non aveva mai ricevuto nulla.

La Suprema Corte, tuttavia, precisa che non contano le risposte fornite dal gestore dei servizi telematici alla richiesta di chiarimenti del difensore dell'appellante che sostiene di non aver ricevuto nulla. Nelle sue argomentazioni, la Corte ribadisce il recente principio secondo cui «*nel regime antecedente alla novella recata dal d.lgs. n. 149 del 2022, la notificazione a mezzo PEC eseguita dall'avvocato ai sensi dell'art. 3-bis della legge n. 53 del 1994 non si perfeziona nel caso in cui il sistema generi un avviso di mancata consegna, anche per causa imputabile al destinatario (come nell'ipotesi di saturazione della casella di PEC con messaggio di errore dalla dicitura "casella piena"), ma soltanto se sia generata la ricevuta di avvenuta consegna (c.d. "RdAC"*)».

Nel caso di specie – tra l'altro – la Corte ha rilevato come fosse pacifico che tale ricevuta fosse stata generata e prodotta tra i documenti depositati dallo stesso ricorrente.

Per questo motivo, la Cassazione ha dichiarato il ricorso inammissibile.

---

23 Gennaio 2025 – Corte Costituzionale: incostituzionali le norme del Codice dell'Amministrazione Digitale (CAD) che hanno l'effetto di impedire ai disabili l'uso della firma digitale per sottoscrivere le liste elettorali.

La Corte Costituzionale ha dichiarato l'illegittimità costituzionale degli artt. 9, terzo comma, della Legge 17 febbraio 1968, numero 108 e 2, comma 6, del Codice dell'amministrazione digitale, nella parte in cui non

prevedono per l'elettore, che non sia in grado di apporre una firma autografa per certificata impossibilità derivante da un grave impedimento fisico o perché si trova nelle condizioni per esercitare il voto domiciliare, la possibilità di sottoscrivere una lista di candidati per le elezioni.

Lo sviluppo tecnologico ha reso inadeguato lo strumento, risalente a quando non esisteva la firma digitale, che prevedeva per i presentatori di una lista di candidati che non erano in grado di sottoscrivere per fisico impedimento, di poter fare la loro dichiarazione in forma verbale, alla presenza di due testimoni, innanzi ad un notaio o al segretario comunale o ad altro impiegato all'uopo delegato dal Sindaco.

Questa procedura, presuppone, infatti «*che i soggetti abilitati a ricevere la dichiarazione verbale e i testimoni si rechino nel domicilio della persona con disabilità, con la conseguenza che a quest'ultima è imposto di attivarsi al fine di ottenere tale presenza, di sostenere gli eventuali oneri economici, e, se del caso, di tollerare una interferenza sulla propria riservatezza*».

In questi termini, conclude la Consulta, «*la preclusione all'utilizzo della firma digitale anche per le persone con disabilità determina il paradosso per cui è l'ordinamento giuridico che, anziché rimuovere gli ostacoli che impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione all'organizzazione politica, introduce esso stesso "un aggravio né necessario, né proporzionato rispetto all'esigenza di verificare l'autenticità e la genuinità della sottoscrizione della lista di candidati, parimenti conseguibile consentendo all'elettore con disabilità di utilizzare la modalità elettronica per sostenere la lista di candidati*"».
