Studio Previti
ASSOCIAZIONE PROFESSIONALE

WEEKLY UPDATE 2025

A CURA DEL DIPARTIMENTO

Compliance, media e tecnologia

La raccolta dei *Regulatory Watch* 2025 riunisce le principali notizie e gli aggiornamenti normativi dell'anno in materia di intelligenza artificiale, compliance e data protection.

Con l'obiettivo di offrire uno strumento di consultazione ancora più completo, viene presentato il lavoro svolto dedicato alle novità introdotte dal pacchetto Omnibus.

In particolare, attraverso il link è possibile accedere e scaricare i materiali relativi: alle proposte di modifica al GDPR, alla Direttiva (UE) 2022/2555 (NIS 2), al Regolamento (UE) 2024/1689 (AI Act) e al Data Act.

Un'integrazione pensata per accompagnare il lettore in un percorso strutturato e aggiornato sulle principali evoluzioni normative del 2025.

CLICCA QUI!

1. Intelligenza artificiale

1.1. Normativa e linee guida

La pubblicazione delle linee guida sulle pratiche vietate dall'AI Act

La Commissione, nel febbraio 2025, ha pubblicato le Linee guida sulle pratiche di AI ritenute inaccettabili, le quali potrebbero causare rischi per i valori e diritti fondamentali europei. Le Linee guida, che contano ben 140 pagine, sono state concepite per garantire un'applicazione coerente, efficace e uniforme dell'AI Act in tutta l'Unione europea, offrendo preziose indicazioni sull'interpretazione dei divieti da parte della Commissione anche attraverso esempi pratici per aiutare le parti interessate a comprendere e rispettare i requisiti normativi.

Link alle Linee Guida

Modelli di AI per finalità generali: pubblicate le linee guida della Commissione

In vista dell'entrata in vigore, a partire dal 2 agosto 2025, degli obblighi imposti ai provider di modelli di IA per finalità generali, la Commissione europea ha pubblicato le Linee guida rivolte ai fornitori di tali modelli (GPAI) con l'obiettivo di dare chiarezza su obblighi e responsabilità lungo tutta la catena del valore, con particolare attenzione a trasparenza, sicurezza informatica e rispetto dei diritti.

Link alle Linee Guida

Legge italiana sull'IA: principi e deleghe al Governo

Il 17 settembre 2025 è stata approvata in via definitiva dal Senato la legge n. 132/2025 sull'Intelligenza Artificiale recante "*Disposizioni e Deleghe al Governo in materia di sull'intelligenza artificiale*" le cui disposizioni si interpretano e applicano conformemente al Regolamento (UE) 2024/1689 (AI Act).

Link alla legge italiana sull'AI

Le linee guida dell'EDPS sull'AI generativa

Nell'ottobre 2025, l'European Data Protection Supervisor (EDPS) ha pubblicato le Linee guida, riviste e aggiornate, sull'utilizzo dell'AI generativa e sulla protezione dei dati personali. L'obiettivo è quello di fornire raccomandazioni e istruzioni pratiche alle istituzioni, agli organi, agli uffici e alle agenzie dell'UE, agevolandone il rispetto degli obblighi in materia di protezione dei dati come stabilito, in particolare, dal Regolamento (UE) 2018/1725.

Link alle Linee Guida

La Guida dell'EDPB per la gestione del rischio dei sistemi di intelligenza artificiale

L'11 novembre 2025, l'EDPB ha pubblicato la "*Guidance for Risk Management of Artificial Intelligence systems*" nella quale ha fornito raccomandazioni pratiche per aiutare l'interprete a identificare e mitigare i rischi tecnici comuni associati ai sistemi di AI, soprattutto nell'ambito della protezione dei dati personali.

Link alla Guida

1.2 Pronunce giurisprudenziali, provvedimenti e sanzioni

Algoritmo di credit scoring e diritto di accesso: prevale il diritto alla spiegabilità

La Corte di Giustizia UE, con sentenza del 27 febbraio 2025 a definizione della causa C-203/22, si è pronunciata sulla questione, oggetto di rinvio pregiudiziale, riguardante il bilanciamento tra il diritto alla tutela del know-how aziendale e il diritto alla protezione dei dati personali dell'individuo, in caso di richiesta di accesso finalizzata ad ottenere informazioni sulle logiche utilizzate dall'algoritmo per la valutazione del merito creditizio (cd. "credit scoring"). La Corte ha chiarito che, ai sensi del GDPR, l'interessato ha diritto a informazioni trasparenti sui dati utilizzati per profilare la sua solvibilità e i parametri per pervenire alla sua valutazione, tuttavia, se il titolare del trattamento ritiene che tali informazioni possano compromettere segreti commerciali, deve sottoporle all'autorità competente per una valutazione del bilanciamento tra trasparenza e tutela delle informazioni riservate.

Link alla sentenza

Addestramento dell'IA di Meta: arriva il monito del Garante Privacy

Nel proprio comunicato stampa del 29 aprile 2025, il Garante Privacy ha ricordato agli utenti il diritto di opposizione al *training* dei sistemi di intelligenza artificiale di Meta, OpenAI, DeepSeek e Google con i propri dati personali. Il Garante si è poi soffermato sul confronto in corso con le altre Autorità nazionali europee per valutare la conformità del trattamento dei dati personali eseguito da parte di Meta sulla base del legittimo interesse.

Link al comunicato stampa del 29 aprile 2025

Trasparenza algoritmica: l'Autorità di Amburgo sanziona una società finanziaria

L'Autorità di controllo di Amburgo, il 30 settembre 2025, ha irrogato ad una società del settore finanziario una sanzione di quasi 500.000 euro per aver impiegato un algoritmo privo di supervisione umana per decidere in merito alle richieste di rilascio di carte di credito e per non aver adempiuto agli obblighi di trasparenza e di informazione previsti dalla normativa in favore degli interessati.

Link al comunicato dell'Autorità di controllo di Amburgo

Experian: credit score in violazione della normativa sulla privacy

Nell'ottobre 2025 l'Autorità olandese ha irrogato a Experian una sanzione di 2,7 milioni di euro per aver violato il GDPR nell'esecuzione e nella successiva fornitura di vari report sul merito creditizio dei consumatori ai propri clienti, tra i quali fornitori di servizi essenziali come l'energia elettrica e le telecomunicazioni. Il trattamento dei dati personali avveniva in assenza di informativa, favorendo un sistema automatico di credit score privo di trasparenza che escludeva gli ignari consumatori da una serie di servizi fondamentali. La vicenda richiama l'importanza del rispetto della normativa privacy e, in particolare, degli obblighi di cui all'art. 22 GDPR.

Link al comunicato dell'Autorità Olandese

Il TAR della Lombardia si pronuncia sull'uso dell'AI nella redazione degli atti giudiziari

Il difensore che negli atti cita giurisprudenza inesistente e/o non pertinente reperita mediante l'impiego di AI viola gli obblighi di lealtà e probità. Ciò è quanto è emerso dalla sentenza n. 3348 del 21 ottobre 2025 con la quale il TAR della Lombardia ha evidenziato l'obbligo per l'avvocato di verificare e controllare l'esito delle ricerche effettuate con AI, nonché il ruolo centrale della decisione umana, come indicato dalla "*Carta dei principi per un uso consapevole dei sistemi di intelligenza artificiale in ambito forense",* redatta dall'Ordine degli Avvocati di Milano nel 2024.

Link alla sentenza n. 3348/2025 del TAR della Lombardia

LinkedIn: *opt out* contro l'addestramento dell'AI

LinkedIn dal 3 novembre 2025 ha annunciato l'utilizzo dei dati personali degli utenti per addestrare i propri sistemi di IA generativa, conseguentemente, il Garante ha pubblicato una scheda informativa per agevolare gli utenti nell'esercizio del diritto di opposizione, dichiarando che coopererà con le altre Autorità al fine di verificare la conformità dell'iniziativa di LinkedIn alla normativa sulla protezione dei dati personali, con particolare riferimento alla legittimità dei meccanismi di opposizione.

Link al comunicato stampa del Garante

Il New York Times contro Perplexity

Il New York Times ha intrapreso un'azione legale contro Perplexity AI, contestando l'uso non autorizzato di articoli protetti da copyright per l'addestramento del modello. La vicenda si inserisce nell'ondata di contenziosi che sta ridefinendo il rapporto tra editoria, AI generativa e diritto d'autore.

Link all'articolo

Mediaset sfida Perplexity: "Prima causa italiana" sull'utilizzo dell'AI

MFE ha citato in giudizio Perplexity AI accusandola di aver utilizzato senza autorizzazione programmi e film del gruppo – tra cui Striscia la Notizia, Le Iene e Tolo Tolo – per addestrare i propri algoritmi. Si tratta della prima azione legale in Italia contro presunte violazioni del diritto d'autore legate all'AI, avviata da RTI e Medusa.

Link alla notizia

2. Telemarketing

Telemarketing: stop ai consensi "*omnibus*" per le chiamate indesiderate

Il Garante Privacy, nel febbraio 2025, ha irrogato una sanzione di 300.000,00 euro alla società Energia Pulita s.r.l. per la violazione di diversi principi del trattamento e la mancata implementazione di misure adeguate a scongiurare il rischio di attivazione di forniture derivanti da contatti illeciti. In particolare, si segnala quanto statuito con riferimento al consenso per la cessione di dati a terzi soggetti genericamente intesi: "*in ragione dell'ampia formulazione utilizzata in ordine alla platea numerosa e indistinta dei cessionari dei dati personali operanti in settori molto differenti tra loro, infatti, l'interessato che voglia ricevere le offerte relative a uno o più delle categorie merceologiche ivi indicate o voglia riceverle tramite uno soltanto dei canali indicati è, di fatto, costretto a conferire un consenso unitario alla cessione indiscriminata dei propri dati a tutti, indistintamente, i soggetti terzi destinatari a scopi promozionali e non è posto nella condizione di esercitare agevolmente i diritti riconosciuti dalla vigente normativa*".

Link al provvedimento

Le misure AGCOM contro telemarketing illecito: il filtro anti-spoofing

AGCOM, con la Delibera 106/25/CONS, ha introdotto dal 19 agosto un filtro anti-spoofing che blocca le chiamate provenienti da rete fissa dall'estero quando viene utilizzato in modo illecito un numero italiano come identificativo del chiamante; una misura che ha già permesso di intercettare milioni di tentativi di traffico fraudolento e che rappresenta un passo significativo nella tutela degli utenti da truffe e telemarketing aggressivo.
Clicca qui per leggere le slide.

Filtro anti-spoofing AGCOM: i primi risultati

L'Autorità, nel settembre 2025, ha pubblicato i primi dati sull'efficacia del filtro anti-spoofing per contrastare le chiamate con numerazioni falsificate: bloccate 43 milioni di chiamate. Un segnale positivo per la tutela dei consumatori e la trasparenza dei servizi di comunicazione elettronica.

Link al comunicato

Dal 19 novembre estensione del blocco anti-spoofing di AGCOM

Dal 19 novembre 2025 il filtro anti-spoofing previsto da AGCOM con la Delibera 106/25/CONS è operativo anche per le numerazioni mobili, ampliando la protezione contro le chiamate ingannevoli e il telemarketing aggressivo basati sulla falsificazione dell'identità del chiamante (CLI Spoofing). La misura ha rafforzato la sicurezza delle comunicazioni elettroniche e richiede agli operatori un adeguamento rapido delle infrastrutture tecniche.
Link alla Delibera di AGCOM

La sentenza della CGUE: chiarimenti per il settore delle comunicazioni elettroniche

La Corte di giustizia dell'Unione Europea, con sentenza del 13 novembre 2025, ha deciso la causa C-654/23 formulando importanti chiarimenti in tema di *soft-spam*: l'indirizzo di posta elettronica di un utente si considera ottenuto dall'editore di una pubblicazione online "nel contesto della vendita di un prodotto o servizio" di cui all'art.13, par. 2 della Direttiva 2002/58/CE, anche nel caso in cui l'utente abbia creato un account gratuito sulla sua piattaforma online che gli consente, non solo l'accesso gratuito a un certo numero di articoli e la ricezione sempre gratuita alla newsletter quotidiana, bensì anche il diritto di accedere, dietro pagamento, ad articoli e servizi aggiuntivi. Inoltre, la Corte ha precisato che nel caso del soft-spam, non sono applicabili le condizioni di liceità del trattamento previste all'articolo 6, paragrafo 1 del GDPR.
Link alla sentenza CGUE C-654/23

Telemarketing: il titolare è responsabile anche in caso di errore umano se viene omessa la formazione dei dipendenti

Il 27 novembre 2025 il Garante Privacy ha comminato una sanzione di 892.738 euro alla società E.ON Energia per aver svolto attività di telemarketing in contrasto con i principi di liceità e responsabilizzazione, in assenza di un'idonea base giuridica, e mettendo in atto misure tecniche e organizzative non adeguate a verificare ed assicurare la corrispondenza tra i consensi resi dagli interessati e le informazioni registrate sui sistemi aziendali.
Link al provvedimento

3. **Tutela dei lavoratori**

Legge 132/2024: lavoro e AI

La Legge 132/2024 è intervenuta anche sull'utilizzo di AI nel contesto lavorativo: sicurezza, affidabilità e trasparenza, rispetto della dignità umana e della riservatezza dei dati personali, obblighi informativi, rispetto dei diritti inviolabili del lavoratore ed istituzione dell'Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro. Sono questi gli elementi sui quali il Legislatore ha puntato per regolamentare l'AI in un settore così delicato come quello lavorativo.
Link alla legge italiana sull'AI

Registrazioni occulte ammesse se necessarie alla difesa

La Corte di Cassazione, con ordinanza n. 20487, pubblicata il 21 ottobre 2025, ha stabilito che è lecito registrare di nascosto le conversazioni tra colleghi se le stesse sono pertinenti e strumentali all'esercizio del diritto di difesa. Occorre, caso per caso, bilanciare tale esigenza con il diritto alla protezione dei dati personali, anche considerando il coinvolgimento di soggetti terzi estranei.
Link alla sentenza

GPS su veicoli aziendali: quando il trattamento integra un controllo illecito del lavoratore?

Con provvedimento del 16 gennaio 2025, il Garante Privacy ha sanzionato con una multa di 50.000,00 euro una società di autotrasporti per controllo illecito dei dipendenti durante l'attività lavorativa mediante un sistema di GPS installato sui veicoli aziendali. L'istruttoria, avviata a seguito del reclamo di un ex dipendente, ha rivelato che il sistema raccoglieva diversi dati, tra cui: informazioni sulla localizzazione, telemetria (velocità e chilometri percorsi), stato del veicolo, messaggi scambiati tra la piattaforma *web* e il dispositivo di bordo, oltre ad eventuali ulteriori informazioni inserite autonomamente dai dipendenti. Il Garante ha riscontrato l'inadeguatezza dell'informativa fornita, segnalando come non riflettesse correttamente le reali modalità di trattamento, e, in più ha accertato una conservazione dei dati eccessiva e non proporzionata rispetto agli scopi dichiarati.
Link al provvedimento

Smart working: il datore non può geolocalizzare i lavoratori

Il datore di lavoro non è legittimato a geolocalizzare i dipendenti nell'ambito dello smart working. A chiarirlo è il Garante Privacy che, a seguito di un reclamo presentato da un dipendente e di una segnalazione da parte dell'Ispettorato della Funzione Pubblica, ha avviato un'istruttoria che ha condotto, con provvedimento del 13 marzo 2025, alla sanzione di 50.000 euro nei confronti di un'azienda che monitorava la posizione geografica dei dipendenti durante lo smart working. In particolare, il personale selezionato per lo svolgimento di attività lavorativa da remoto veniva contattato telefonicamente dall'Ufficio controlli per richiedere l'attivazione della geolocalizzazione del computer o dello smartphone. Una volta completata tale operazione, si procedeva alla timbratura su una specifica applicazione e, a seguire, il dipendente doveva inviare una dichiarazione sul luogo in cui si trovava il dipendente.

Link al provvedimento

Regione Lombardia sanzionata per controllo dei dipendenti in violazione del GDPR

Il Garante per la protezione dei dati personali, con provvedimento del 29 aprile 2025, ha deliberato una sanzione pecuniaria pari a 50mila euro nei confronti Regione Lombardia, avendo riscontrato diverse violazioni della normativa vigente in materia di protezione dei dati personali dei dipendenti e dei limiti al controllo datoriale: raccolta e conservazione dei log di navigazione in internet riguardo alle informazioni di siti web visitati dai dipendenti, inclusi quelli inseriti nella black list, in mancanza di un accordo collettivo con le rappresentanze sindacali di adeguate garanzie a tutela del lavoratore.

Link al provvedimento

WhatsApp aziendale e privacy dei dipendenti: serve il consenso

L'Autorità spagnola per la privacy (AEPD), nel giugno 2025, ha stabilito che aggiungere i lavoratori attraverso il proprio numero privato in chat di gruppo aziendale su WhatsApp senza consenso esplicito è una violazione della loro privacy: sanzionato per 70.000 euro il datore di lavoro (una nota società che gestisce marchi di alta moda). Le aziende devono impiegare canali ufficiali e policy dedicate per le comunicazioni interne, evitando condotte che potrebbero violare la privacy dei dipendenti.

Link al provvedimento dell'AEPD.

Trasparenza retributiva: nuove regole UE e impatti per le aziende

La Direttiva UE 2023/970, che dovrà essere recepita dagli Stati Membri entro il 7 giugno 2026, ha introdotto obblighi di trasparenza salariale per combattere la disparità retributiva tra uomini e donne,

con particolare attenzione al "gender pay gap", che in Europa si aggira attorno al 13%: criteri retributivi chiari e accessibili da parte delle aziende, divieto di clausole di riservatezza sui salari e informazioni trasparenti ai lavoratori sulle retribuzioni medie per genere, ruolo e mansione.
Link alla Direttiva UE 2023/970

3. Tutela dei minori

EDPB: quali novità in tema di "*age assurance*" e IA?

Nel corso della sua riunione plenaria del 12 febbraio 2025, l'European Data Protection Board ha comunicato di aver adottato una "*dichiarazione sulla garanzia dell'età*" e di voler procedere all'estensione dell'ambito di applicazione della task force creata per monitorare la conformità di ChatGPT verso un controllo più generale dell'IA. Nella dichiarazione l'EDPB ha elencato dieci principi per determinare, lecitamente, l'età o la fascia di età di una persona, con la speranza di apportare un approccio europeo coerente tra l'esigenza di proteggere i minori e quella di rispettare i principi in ambito data protection.
Link al comunicato

Age Verification: l'AGCOM approva le regole per la verifica della maggiore età degli utenti online

Con l'adozione della delibera 96/25/CONS l'AGCOM, dopo aver acquisito il parere favorevole del Garante per la protezione dei dati personali, ha imposto alle piattaforme di condivisione video e i siti web con contenuti potenzialmente inadatti ai minori di adottare entro 6 mesi sistemi certificati di verifica della maggiore età. In attuazione del Decreto Caivano e delle disposizioni contenute nel Digital Services Act (DSA) in materia di sicurezza online, l'AGCOM ha adottato delle nuove regole che impongono alle piattaforme che ospitano contenuti (es: materiale pornografico, gioco d'azzardo) e prodotti (es: alcolici e tabacco) inadatti ai minori di implementare entro ottobre un meccanismo di age verification basato sul "*doppio anonimato*".
Link al comunicato

Asilo sanzionato per violazione della privacy dei minori

Il Garante, con provvedimento del 10 luglio 2025, nel principio del superiore interesse del minore, ha sanzionato per 10 mila euro un asilo per aver subordinato l'iscrizione al rilascio del consenso da parte dei genitori alla pubblicazione delle immagini dei propri figli online e aver adottato un sistema di videosorveglianza in violazione della normativa privacy de dello Statuto dei lavoratori.

Link alla News

Disney multata per violazioni della privacy dei minori su YouTube

La Disney si è accordata con la FTC per pagare 10 milioni di dollari in risposta all'accusa di aver pubblicato video su YouTube indirizzati ai bambini, ma senza contrassegnarli come tali. Una raccolta non autorizzata di dati di minori in assenza di informativa e dell'acquisizione del necessario consenso da parte dei genitori. Violato anche il *Children's Online Privacy Protection Rule* (COPPA) che riconosce ai genitori il potere di assumere decisioni per i propri figli e, non di certo, alle aziende. La Compagnia ora deve attivare programmi di revisione dei contenuti e conformarsi al dettame normativo.

Link alla News

Audizione del Garante sul disegno legge 1336

Il 7 ottobre 2025, il Presidente del Garante per la protezione dei dati personali si è pronunciato sul Disegno di Legge 1336 relativo alla tutela dei minori nella dimensione digitale. Attivazione degli *account social* ammessa per i soli ultraquindicenni, dubbi sulla soglia dell'età per il consenso digitale elevata a sedici anni e sulla limitazione della possibilità di prestare il consenso genitoriale al trattamento dei minori alla sola fascia compresa tra i quindici e sedici anni, possibilità di attribuire all'Autorità il potere di inibire i servizi che violano la normativa privacy: sono questi gli aspetti principali emersi dall'Audizione del 7 ottobre.

Link alla News

California: protezione dei minori e AI

Nell'ottobre del 2025 il governatore Gavin Newsom ha firmato una legge "storica" che rafforza ulteriormente le tutele dei minori nelle piattaforme online e nell'uso dell'AI. Tra gli strumenti: verifica dell'età obbligatoria, chatbot che rispettano protocolli ad hoc per tematiche relative al suicidio e all'autolesionismo, trasparenza dell'interazione con l'AI, divieto di chatbot "*professionisti sanitari*", avvertimenti sui danni associati all'uso prolungato dei social, sanzioni più severe per i deepfake pornografici, linee guida contro il cyberbullismo e impossibilità di imputare la responsabilità all'AI escludendo quella umana. Un pacchetto normativo che pone al centro la tutela del minore.

Link alla News

AGCOM: *Age verification* per i siti e le piattaforme che diffondono contenuti pornografici

Dal 12 novembre 2025 sono entrate in vigore gli obblighi AGCOM di verifica dell'età per siti e piattaforme che diffondono contenuti pornografici in Italia. Il mancato adeguamento può comportare sanzioni fino a 250.000 euro e l'impossibilità di proseguire la diffusione dei servizi.
Link alla notizia

L'aggiornamento della guida "Social media" del Garante

Il 14 novembre 2025, l'Autorità ha pubblicato una versione aggiornata della guida dedicata all'utilizzo dei social. Si approfondiscono temi legati alla tutela dei minori, alla profilazione, alla trasparenza e anche ai rischi di revenge porn e cyberbullismo. Il Garante offre, inoltre, indicazioni operative e consigli pratici agli utenti al fine di fare un uso più consapevole e sicuro delle piattaforme digitali.
Link al comunicato del Garante

4. Videosorveglianza

L'avvertimento del Garante a CamHub

Il Garante, con comunicato stampa del 6 ottobre 2025, ha rivolto un avvertimento formale a CamHub per la raccolta e diffusione di video estratti abusivamente da telecamere presenti in luoghi privati. La divulgazione di contenuti privati è suscettibile di causare un pregiudizio grave e irreparabile agli interessati. L'Autorità ha evidenziato come sia fondamentale implementare misure di sicurezza adeguate nei i circuiti di videosorveglianza privati, così da evitare l'accesso libero e non autorizzato ai dati personali.
Link alla News

Tempi di conservazione della videosorveglianza

Il Consiglio di Stato, con sentenza n. 8472 del 31 ottobre 2025, pronunciandosi sul rapporto tra conservazione delle immagini raccolte tramite sistema di videosorveglianza e diritto d'accesso dell'interessato, ha chiarito la legittimità del diniego opposto dal Comune alla richiesta d'accesso alle immagini e video da parte dell'interessato, se giustificato dal regolamento dell'ente che limita a pochi giorni (nel caso cinque) la conservazione dei dati, tenuto conto delle esigenze di difesa e accertamento degli illeciti, dell'interesse pubblico alla sicurezza ambientale e stradale, nonché dei principi del GDPR.
Link alla sentenza

Videosorveglianza: Comune sanzionato per illegittimo trattamento dei dati raccolti

Con il provvedimento del 19 dicembre 2024 il Garante ha sanzionato con una multa di 4.000 euro il Comune di Levanto per aver installato alcune telecamere dotate di funzionalità di lettura automatizzata delle targhe dei veicoli in transito senza preventivamente effettuare una valutazione di impatto e senza l'autorizzazione necessaria della Prefettura.
L'istruttoria ha accertato la conservazione delle targhe ingiustificatamente ben oltre il limite dei sette giorni di cui all'art. 6 del D.L. 11/2009 (180 giorni); oltre ad un'informativa difficilmente accessibile
Link al provvedimento

Furto sul luogo del lavoro da parte: le riprese del datore non violano la privacy del dipendente

Con la sentenza n. 3045 del 6 febbraio 2025, la Corte di Cassazione ha confermato la legittimità dei controlli difensivi sui dipendenti per la tutela del patrimonio aziendale con esclusione di qualsiasi violazione della privacy del dipendente coinvolto.
La Suprema Corte ha evidenziato che, nel caso di specie, da un lato le riprese erano finalizzate alla tutela del patrimonio aziendale e non al controllo diretto dell'attività lavorativa, nel pieno rispetto dell'art. 4, dello Statuto dei Lavoratori; dall'altro lato il lavoratore non era specificamente controllato, ma semplicemente investito dal raggio d'azione delle telecamere di videosorveglianza mentre svolgeva il suo lavoro all'esterno.
Link alla sentenza

5. Deepfake

Inghilterra: nuove leggi contro i "deepfake" per proteggere donne e ragazze online

Il governo britannico ha annunciato, con comunicato stampa del 7 gennaio 2025, l'introduzione di nuovi reati volti a combattere la creazione e la condivisione di immagini "deepfake" sessualmente esplicite senza consenso dei soggetti coinvolti, con pene detentive fino a due anni, compreso lo scatto di immagini intime senza consenso e l'utilizzo di tool per commettere tali reati.
Lo scopo è quello di contrastare la proliferazione di abusi online, proteggendo in particolare donne e ragazze, spesso vittime di tali atti.
Link al comunicato

La truffa con il falso Ministro Crosetto ha generato preoccupazioni sull'uso criminale dell'intelligenza artificiale

Un gruppo di truffatori ha utilizzato le tecnologie dell'IA per clonare la voce del ministro della difesa Guido Crosetto, ingannando diversi imprenditori e convincendoli a versare ingenti somme di denaro su conti esteri. Tale episodio ha evidenziato i rischi legati all'uso illecito dell'intelligenza artificiale in grado di manipolare voce e immagine, portando ad una seria difficoltà di distinzione tra reale e falso, facilitando le truffe. Questo caso non ha potuto fare a meno di far riaccendere dei dibattiti sulla necessità di regolamentare l'uso dell'IA. Infatti, oltre all'AI ACT è noto che il DDL 1146/2024 sull'intelligenza artificiale in Italia prevede l'introduzione di reati specifici per l'utilizzo illecito dell'intelligenza artificiale ai fini della creazione di "deepfake".
Link alla notizia

Socialmediagirls: deepfake e deepnude

Nell'ottobre 2025 si è ritornati a discutere di deepfake e deepnude per *Socialmediagirls*, il forum online in cui sono pubblicate immagini intime generate con AI che ha coinvolto numerosi personaggi pubblici. Non solo i dati personali, ma anche la dignità e la reputazione delle persone sono a rischio. L'introduzione del reato di cui all'art. 612 quater c.p., ad opera della legge 132/2025, è indubbiamente uno strumento utile per contrastare tale fenomeno.
Link alla notizia

Il controllo preventivo degli annunci da parte del gestore di un market online

La Corte di giustizia dell'Unione Europea, con sentenza del 2 dicembre 2025 a definizione della causa C-492/23, ha chiarito che il gestore di un mercato online, in quanto titolare del trattamento dei dati personali contenuti negli annunci ivi pubblicati, è tenuto, prima della pubblicazione, e mediante misure tecniche e organizzative adeguate, a individuare gli annunci che contengono dati sensibili ex art. 9 par. 1 GDPR, a verificare se tali dati siano dell'utente inserzionista e, in caso contrario, a rifiutare la pubblicazione, salvo che quest'ultimo possa dimostrare che la persona interessata abbia prestato il proprio consenso esplicito o che il trattamento possa fondarsi su una delle basi giuridiche di cui all'art. 9, par. 2 GDPR .
Link alla sentenza

Il dipartimento *Compliance, media e tecnologia*

Il dipartimento offre consulenza legale in materia di privacy, intelligenza artificiale, IT, comunicazione e compliance aziendale, supportando le aziende nel rispetto del GDPR e nei progetti di digitalizzazione.

Fornisce assistenza anche nella gestione delle tecnologie emergenti e nella relazione con le autorità competenti. Inoltre, aiuta le imprese a sviluppare strategie di cyber resilienza attraverso valutazioni di maturità e piani personalizzati di miglioramento della sicurezza informatica.

Studio Previti

ASSOCIAZIONE PROFESSIONALE

contatti@previti.it
www.previti.it

06.3234623
02.795587

Via Cicerone, 60 00193 Roma
Via Stradivari, 4 20131 Milano