

Rassegna di novità in materia di diritto penale e nuove tecnologie

Responsabile scientifico: Prof. Lorenzo Picotti – monitoraggio e redazione a cura di Chiara Crescioli (C.C.), Stefano Dolci (S.D.), Beatrice Panattoni (B.P.), Lisa Perobello (Li.Pe.), Simone Tarantino (S.T.), Rosa Maria Vadalà (R.M.V.) e Lorenzo Picotti (L.P.).

NOVITÀ SOVRANAZIONALI

1. Regolamento (UE) 2026/1744 del Parlamento Europeo e del Consiglio: modifica ai regolamenti che riguardano l'attuazione delle regole sull'Intelligenza Artificiale (Digital Omnibus AI)

Il regolamento del Parlamento europeo e del Consiglio dell'8 luglio 2026, pubblicato in GUUE il 24 luglio 2026 ed **entrato in vigore il 27 luglio 2026**, nasce dalla proposta della Commissione COM (2025) 836 del 19 novembre 2025, nell'ambito del settimo pacchetto di semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale, contenute in particolare nell'*AI Act* (regolamento UE 2024/1689).

I termini della sua applicazione sono stati in particolare posticipati al 2 dicembre 2027 per le disposizioni dell'art. 6 e correlate regole concernenti i sistemi “*ad alto rischio*”. Il nuovo regolamento comporta altresì la riduzione di oneri amministrativi, il rafforzamento di alcuni divieti, la spiegazione relativa all'applicazione concreta di alcune norme e la precisazione delle materie di competenza dell'*AI Office*.

Di particolare rilievo è l'ampliamento del catalogo delle pratiche vietate di cui all'art. 5 dell'*AI Act*, con l'introduzione delle lettere *b-bis*) e *b-ter*) al paragrafo 1. Viene vietata l'immissione sul mercato, la messa in servizio o l'uso di sistemi di intelligenza artificiale che generano o manipolano immagini, video o audio realistici raffiguranti le parti intime di una persona fisica riconoscibile, o la stessa mentre compie atti sessualmente espliciti, in assenza del consenso libero, specifico, informato e inequivocabile della persona ritratta (c.d. *deepfake*, materiale intimo non consensuale, generato soprattutto da applicazioni di IA che consentono la “nudificazione”). Si tratta infatti di materiale lesivo dei diritti fondamentali delle persone, che costituisce una forma di violenza e abuso sessuale soprattutto nei confronti di donne e minori. È per questo parimenti vietata l'immissione sul mercato, la messa in servizio o l'uso di sistemi che generano o manipolano materiale o spettacoli ai sensi dell'art. 2, lettere c) ed e), della direttiva 2011/93/UE, e dunque materiale di abuso sessuale su minori, incluso quello integralmente o parzialmente sintetico, salva l'applicabilità di una causa di giustificazione prevista dal diritto nazionale ai sensi dell'art. 5, paragrafo 1, della medesima direttiva (utilizzo di materiale di abuso sessuale sui minori da parte delle autorità nazionali per condurre attività di contrasto, prevenzione, indagine o *red teaming*).

Quanto alla portata degli obblighi per i fornitori di servizi e per i *deployer*, il regolamento (UE) 2026/1744, che introduce il nuovo art. 5, paragrafo 1-bis, dell'*AI Act*, circoscrive la responsabilità del fornitore ai casi in cui la generazione o manipolazione di tale materiale costituisca la finalità prevista del sistema, ovvero un risultato ragionevolmente prevedibile e riproducibile in assenza di misure tecniche di sicurezza adeguate (tra cui la pulizia dei dati di addestramento, l'addestramento al rifiuto, i controlli sull'output e i meccanismi di rilevamento dell'abuso).

La responsabilità del *deployer*, per converso, sorge unicamente laddove questi utilizzi effettivamente il sistema per generare o manipolare il materiale vietato, restando esclusi sia l'uso lecito di sistemi privi delle garanzie che il fornitore avrebbe dovuto predisporre, sia la generazione o manipolazione meramente accidentale. Il paragrafo 1-ter esclude dalla nozione di “manipolazione” il mero miglioramento tecnico di materiale preesistente che non ne accresca il livello di esposizione delle parti intime né alteri la natura degli atti sessualmente espliciti raffigurati.

Le violazioni degli obblighi imposti ai fornitori di servizi e ai *deployer* comportano l'applicazione delle severe sanzioni amministrative ai sensi dell'art. 99 dell'*AI Act*, ma, come evidenziato al considerando 15 del regolamento (UE) 2026/1744, possono integrare altresì distinte fattispecie di reato previste dalla normativa degli Stati membri e dalle direttive 2011/93/UE e (UE) 2024/1385. Per questo motivo il regolamento ricorda il rispetto del principio del *ne bis in idem* di cui alla Carta dei diritti fondamentali dell'Unione europea (**Li.Pe.**)

Il testo del Regolamento 2026/1744 è disponibile al seguente [link](#).

2. *European Technological Sovereignty Package*: nuovo pacchetto per l'indipendenza e l'innovazione tecnologica europea

In data 3 giugno 2026 la Commissione europea ha trasmesso al Parlamento un pacchetto in ambito di sovranità tecnologica. L'obiettivo è rafforzare l'autonomia strategica europea nei settori tecnologici considerati essenziali quali, semiconduttori, *cloud*, intelligenza artificiale, *software* e infrastrutture digitali, riducendo la dipendenza da fornitori extra-UE, in particolare statunitensi e cinesi. Il pacchetto riunisce quattro iniziative, due legislative e due di natura strategica.

Il primo pilastro è la proposta *Chips Act 2.0*, che aggiornerà il regolamento (UE) 2023/1781. L'obiettivo è rafforzare l'intera filiera europea dei semiconduttori, incrementando la capacità produttiva dell'Unione, sostenendo la progettazione e la produzione di *chip* avanzati, migliorando la resilienza delle catene di approvvigionamento e stimolando la domanda di componenti europei. La proposta prevede inoltre nuovi strumenti di coordinamento tra gli Stati membri, un rafforzamento della governance europea del settore e misure per attrarre investimenti pubblici e privati.

Il secondo pilastro è il *Cloud and AI Development Act (CADA)*, che costituisce probabilmente la parte più innovativa del pacchetto. La proposta è volta allo sviluppo della ricerca e dell'innovazione di tecnologie all'avanguardia e sostenibili, bilanciando al contempo le ambizioni di intelligenza artificiale con gli impegni climatici. La proposta mira a creare un ecosistema europeo del *cloud* e dell'intelligenza artificiale, con particolare attenzione alle strutture altamente sostenibili ed innovative, attraverso:

- il sostegno alla realizzazione di nuovi *data center*;
- l'accelerazione delle infrastrutture necessarie allo sviluppo dell'AI;
- un quadro comune europeo per valutare la "sovranità" dei servizi *cloud*;
- criteri uniformi per individuare fornitori affidabili nelle infrastrutture critiche;
- misure volte a ridurre la dipendenza dai grandi operatori extraeuropei.

L'idea di fondo è che il controllo dell'infrastruttura digitale costituisca un elemento essenziale della sicurezza economica e della sovranità tecnologica dell'Unione.

Il terzo pilastro non introduce nuovi obblighi giuridici, ma definisce una strategia per promuovere l'utilizzo di *software open source*. La Commissione ritiene che una maggiore diffusione di soluzioni aperte possa ridurre il fenomeno del *vendor lock-in*, favorire l'interoperabilità, rafforzare la sicurezza informatica e aumentare la capacità europea di controllare le tecnologie impiegate nelle amministrazioni pubbliche e nei servizi essenziali. La strategia prevede investimenti nelle competenze, nel sostegno alle *start-up* e nello sviluppo di infrastrutture digitali aperte.

L'ultimo pilastro riguarda il rapporto tra transizione digitale e sistema energetico. La Commissione evidenzia che lo sviluppo dell'AI comporterà una crescita significativa della domanda di energia, soprattutto per effetto dei *data center*. Per questo propone una *roadmap* che favorisca l'integrazione sostenibile dei *data center* nella pianificazione energetica europea, l'impiego dell'AI nella gestione delle reti e lo sviluppo di modelli di AI sicuri e che rendano il sistema energetico europeo più efficiente.

Al di là delle singole iniziative, il pacchetto riflette un cambiamento di prospettiva della politica europea. Negli ultimi anni l'UE si è concentrata prevalentemente sulla regolazione del mercato digitale (con strumenti quali il *Digital Markets Act*, il *Digital Services Act* e l'*AI Act*), con il pacchetto sulla sovranità tecnologica, invece, l'attenzione si sposta anche sul rafforzamento della capacità industriale europea, attraverso investimenti, infrastrutture e politiche di sostegno alla produzione tecnologica sostenibile. L'obiettivo dichiarato è consentire all'Unione Europea di sviluppare e controllare tecnologie strategiche, preservando la propria autonomia senza rinunciare all'apertura dei mercati. (**Li.Pe.**)

I documenti sono consultabili al seguente [link](#).

3. *EUROPOL*: Report sulle minacce e le tendenze in evoluzione nel panorama della criminalità informatica

Con il report *Internet Organised Crime Threat Assessment*, l'Europol rileva come l'accessibilità crescente degli strumenti di intelligenza artificiale consenta più facilmente ai criminali informatici di violare le disposizioni

normative con conseguente aumento delle operazioni illecite, riducendo al contempo il coinvolgimento diretto degli autori materiali nelle singole condotte. La diffusione di piattaforme a crittografia *end-to-end* (E2EE), unita a barriere giurisdizionali e a politiche di *data retention* non armonizzate tra i fornitori di servizi *online*, genera significativi punti ciechi investigativi, ostacolando l'identificazione dei sospetti e la raccolta delle prove. In tale contesto, le frodi *online* costituiscono il settore della criminalità organizzata a crescita più rapida, che con lo strumento del *ransomware*, con oltre 120 varianti attive censite da Europol nel 2025, evolve verso modelli di estorsione fondati sulla minaccia di divulgazione dei dati.

Sul fronte dello sfruttamento sessuale dei minori *online*, l'impiego di AI generativa e di piattaforme E2EE aggrava le difficoltà di individuazione delle vittime e di repressione dei reati. Il report raccomanda pertanto alle Autorità Governative un investimento proattivo finalizzato all'implementazione delle conoscenze in tema di intelligenza artificiale, l'armonizzazione delle politiche di conservazione dei dati e un rafforzamento della cooperazione con il settore privato, quale presupposto per colmare il divario di velocità tra evoluzione della minaccia e capacità di risposta istituzionale. **(Li.Pe.)**

Il report è disponibile al seguente [link](#).

4. Latitante arrestato in Spagna grazie alla piattaforma UE Most Wanted

Grazie alla piattaforma denominata *UE Most Wanted*, sito lanciato nel 2016 dalla *Rete Europea delle Squadre di Ricerca Attiva dei Fuggitivi* (ENFAST), è stato possibile rintracciare un latitante ungherese ricercato per aver commesso delitti a sfondo sessuale a danno di un minore.

L'uomo, il cui profilo era stato aggiunto alla piattaforma soltanto tre giorni prima, è stato arrestato in Spagna lo scorso 7 maggio, a dimostrazione dell'efficacia e delle tempestività di questo mezzo, il quale fornisce, infatti, un dettagliato elenco dei soggetti indagati o condannati in Europa per reati di particolare gravità, consentendo, così, a chiunque di poter effettuare segnalazioni alle forze dell'ordine. **(S.D.)**

La notizia è disponibile al seguente [link](#).

5. INTERPOL: nuovo report sull'escalation della criminalità informatica

Il report *Asia and South Pacific Cyber Threat Assessment Report 2025/2026* pubblicato da Interpol *Asia and South Pacific Cybercrime Desk* (ASP Desk), nell'ambito del progetto ASPJOC (*Asia and South Pacific Joint Operations against Cybercrime*, finanziato dal Regno Unito), fotografa lo stato della criminalità informatica nella regione asiatica tra gennaio 2024 e marzo 2025, sulla base di un questionario sottoposto a 18 Paesi membri e di dati tecnici forniti da partner privati. Il rapporto rileva, in primo luogo, l'industrializzazione delle truffe *online* gestite da organizzazioni criminali transnazionali attive in Cambogia, Laos, Myanmar e Filippine attraverso veri e propri *scam center*, ossia enormi complessi industriali e urbani, dove migliaia di persone sono costrette a compiere truffe informatiche *online* su scala globale. Le organizzazioni criminali fanno ampio ricorso al lavoro forzato (assimilato a forme di schiavitù moderna) e generano proventi stimati in circa 40 miliardi di dollari USA l'anno.

Nel report viene altresì documentato l'aumento degli attacchi *ransomware* (oltre 135.000 nel 2024) e delle intrusioni DDoS (+92%), nonché la diffusione di *malware infostealer* (RedLine, LummaC2, Lokibot, tra i più rilevati nella regione), utilizzati per sottrarre credenziali e dati finanziari, spesso prodromici a frodi su più larga scala.

Un capitolo specifico è poi dedicato al ruolo dell'intelligenza artificiale generativa come fattore di amplificazione delle minacce. In particolare, si analizza l'utilizzo dei *deepfake* impiegati per impersonare dirigenti aziendali richiedendo il pagamento di ingenti somme ai dipendenti dell'azienda vittima dei truffatori. I *deepfake* vengono inoltre utilizzati nelle cd truffe *romance baiting scams* (con perdite stimate fino a 37 miliardi di dollari USA), nonché per la realizzazione di contenuti artificiali a sfondo sessuale.

A fronte di tale scenario, il report dà conto, distintamente, di due livelli di risposta. Da un lato, descrive le misure recentemente adottate da singoli Stati membri: tra queste, l'inasprimento sanzionatorio in materia di materiale sessuale *deepfake* in Corea del Sud, il potenziamento della *Cybercrime Directorate* indonesiana, la nuova regolamentazione dei prestatori di servizi su cripto-attività a Hong Kong e la messa al bando nazionale dei *Philippine Offshore Gaming Operators* (POGO) nelle Filippine. Dall'altro lato, illustra la strategia

dell'Interpol nell'ambito del più ampio *Strategic Framework 2026-2030 (Together Against Crime)*. Il *Global Cybercrime Programme* è strutturato in tre pilastri operativi che prevedono lo sviluppo di un sistema di controllo delle cyber minacce, delle capacità investigative dei Paesi membri, nonché la conduzione di operazioni transnazionali coordinate, in continuità con quanto già posto in essere con la c.d. operazione *SECURE* (febbraio 2025), che ha coinvolto 26 Stati e portato alla disattivazione di oltre 20.000 indirizzi IP e domini malevoli collegati a campagne di *infostealer*. (**Li. Pe. e S. D.**)

Il testo del report è consultabile al seguente [link](#).

6. EUROPOL e EUROJUST: Conferenza del 24.6.2026 sull'operazione coordinata per bloccare reti criminali informatiche

Con un'operazione denominata Operazione *Endgame*, coordinata da Europol e Eurojust che ha visto il coinvolgimento di più Stati, quali Canada, Danimarca, Germania, Paesi Bassi, Regno Unito, Stati Uniti e società di software private, come Microsoft, sono state interrotte le cosiddette “catene di montaggio” che i cybercriminali usano per lanciare *ransomware*, frodi finanziarie e attacchi alle infrastrutture critiche. Questa operazione ha segnato un cambiamento di strategia: invece di concentrarsi esclusivamente sulle minacce individuali, Europol, le forze dell'ordine e le autorità giudiziarie, così come partner privati del settore, hanno interrotto l'intera catena che permetteva agli attacchi informatici di avere successo, contaminando siti web con malware o estraendo informazioni sensibili come *password*, dati di accesso memorizzati e identità digitali da computer compromessi, rendendole disponibili per un successivo uso illecito, in particolare il commercio e l'utilizzo di dati personali. (**Li.Pe.**)

Il rapporto dell'Europol è consultabile al seguente [link](#).

7. COMMISSIONE EUROPEA: Europol ed Eurojust rafforzati per intensificare la lotta contro la criminalità transfrontaliera e il terrorismo

La Commissione europea propone l'adozione di nuove misure per implementare la risposta dell'Unione ad un panorama di criminalità organizzata sempre più transfrontaliero, sofisticato ed organizzato, che sfrutta una rete digitale capace di interconnettersi in un ecosistema che combina le infrastrutture digitali, i flussi finanziari illeciti ed i servizi online. A fronte di uno scenario così descritto, ne discende la necessità di un approccio combinato tra Stati, anche grazie all'intervento dell'Unione.

Le proposte mirano a creare un coordinamento tra gli organi giurisdizionali di ogni Stato membro (polizia giudiziaria ed amministrativa, dogana, pubblici ministeri) dalla genesi delle indagini, passando per l'accertamento, la prevenzione, la cooperazione giudiziaria e l'azione penale efficace, fino all'accertamento della responsabilità degli autori con sentenza definitiva.

In particolare, si intendono ampliare due strumenti affidati all'UE: l'Europol e l'Eurojust.

Quanto **all'Europol**, quale centro dell'UE per la cooperazione di polizia nell'attività di contrasto, questo sosterrà gli Stati membri garantendo: **i)** uno scambio di informazioni più efficace, veloce e sicuro, tramite un'infrastruttura cloud ed uno spazio condiviso di dati di polizia; **ii)** maggiore sostegno operativo agli Stati membri, mediante uffici di Europol con personale esperto in cybercriminalità; **iii)** un polo tecnologico ed innovativo per la lotta sistemica alla criminalità organizzata; **iv)** una cooperazione più stretta con gli organi e gli organismi dell'UE (in *primis*, Procura europea ed Eurojust); **v)** una cooperazione internazionale rafforzata con i Paesi extra-Ue, per contrastare congiuntamente la criminalità transfrontaliera.

Quanto **all'Eurojust**, quale Agenzia dell'Unione per la cooperazione giudiziaria penale, questa sosterrà le Autorità degli Stati membri, mediante: **i)** il rafforzamento delle capacità organizzative e dell'intervento operativo; **ii)** una lotta serrata alle sfere di criminalità emergenti, in specie quella informatica; **iii)** il rafforzamento della governance e del processo decisionale, specie nei casi più gravi laddove è urgente dare una risposta unitaria forte; **iv)** la creazione di un sistema integrato di giustizia penale dell'Unione, che coopererà con la Procura europea ed Europol, mediante interscambio di flussi informativi sui casi rilevanti; **v)** il potenziamento dell'impegno di cooperazione internazionale, che comporti il coinvolgimento anche di Paesi extra-Ue.

La Commissione propone, inoltre, di rafforzare l'ordine europeo di indagine e di introdurre un nuovo ordine europeo di partecipazione a distanza, per consentire alle Parti processuali di partecipare da remoto alle udienze penali che si svolgono in altro Stato membro.

Infine, la Commissione propone anche di aggiornare il regolamento sulla protezione dei dati trattati dalle Istituzioni, dagli Organi e dagli Organismi dell'Unione (EUDPR), per garantire una più efficace cooperazione tra le istituzioni, gli organi e gli organismi di giustizia penale dell'UE, estendendola fra l'altro all'EPPO (S.T.).

Comunicato stampa della Commissione europea rinvenibile al seguente [link](#).

8. CONSIGLIO DELL'UNIONE EUROPEA: lotta contro l'abuso sessuale su minori: l'UE concorda norme di diritto penale più rigorose e un maggiore sostegno per le vittime

La Presidenza del Consiglio ed i Rappresentanti del Parlamento europeo hanno raggiunto un accordo provvisorio di Direttiva, che sia d'impulso all'aggiornamento delle norme di diritto penale dell'UE in materia di tutela dei minori da ogni forma di abuso e sfruttamento, perpetrato anche mediante il ricorso agli sviluppi tecnologici adibiti alla commissione dei crimini.

L'accordo prevede l'aggiornamento delle norme preesistenti, che riformi il quadro normativo risalente alla direttiva 2011/93, con l'introduzione di specifiche fattispecie volte a punire l'abuso o lo sfruttamento perpetrato mediante gli strumenti informatici e telematici. In particolare, per rispondere in modo deciso all'allarmante crescita della condivisione di contenuti pedopornografici realizzati mediante le IA tramite i c.d. *deep fake* (su cui cfr. *supra sub 1.*) si intende rendere punibile “il pagamento per accedere alla trasmissione in diretta di abusi sessuali su minori”, la “progettazione o l'adattamento dei sistemi di AI per produrre materiale pedopornografico”, compresa la distribuzione di questi sistemi.

La normativa interviene anche sul fenomeno dell'adescamento *online*, ossia l'incitamento di un minore che non ha raggiunto l'età del consenso sessuale a “produrre o condividere” materiale pedopornografico, il quale sarà oggetto di specifica fattispecie penale.

Inoltre, tra le innovazioni rilevanti può apprezzarsi la criminalizzazione del possesso e della diffusione di istruzioni, manuali e *prompt* finalizzati alla realizzazione di contenuti pedopornografici tramite applicativi come agenti virtuali, già in uso di tutti.

Le norme interverranno anche in tema di consenso del minore che ha raggiunto l'età della maturità sessuale, dovendo questo essere espresso, inequivoco, chiaro, libero da condizionamenti ed evidente. Al contrario, il consenso deve ritenersi insussistente quando il minore non acconsenta volontariamente sulla base della sua libera volontà o quando questa non può ritenersi valida in quanto coartata o estorta, comunque resa, mediante inganno o persuasione.

In ogni caso, resta fermo che la definizione normativa dell'età del consenso sessuale, vale a dire l'età al di sotto della quale è vietato compiere atti sessuali con un minore, rimane di competenza nazionale.

Anche l'aumento del tempo previsto per perseguire taluni gravi reati commessi nei confronti dei minori dopo il compimento della maggiore età della vittima, dovrà essere esteso. L'ipotesi “*arriva fino a 32 anni per lo stupro di minori di età inferiore e superiore all'età del consenso sessuale e per aver costretto un minore a prostituirsi*”.

Infine, dovrà essere migliorato il sostegno alle vittime minori di abuso e sfruttamento sessuale, mediante potenziamento delle “*linee telefoniche di assistenza*”, che informeranno le vittime ed i familiari degli strumenti a loro disposizione, oltre che garantire un accesso tempestivo e gratuito ai servizi sanitari ed al patrocinio per i non abbienti.

L'accordo provvisorio deve ora essere approvato dal Consiglio e dal Parlamento, per poi essere adottato formalmente dalle due Istituzioni, dopo la messa a punto da parte dei giuristi-linguisti (S.T.).

Comunicato stampa n. 529/2026 del 22 giugno 2026 reperibile al seguente [link](#).

1. Le disposizioni penali contenute nel d.lgs. 9 settembre 2026, n. 160 di attuazione delle deleghe contenute nell'art. 24 l. 23 settembre 2025, n. 132 in materia di intelligenza artificiale.

È stato pubblicato nella Gazzetta Ufficiale n. 214 del 15 settembre 2026, entrando dunque in vigore dal 30 settembre 2026, il decreto legislativo delegato dall'art. 24 della legge italiana sull'intelligenza artificiale n. 132 del 2025, che non si limita a completare l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2024/1689, c.d. *AI Act*, ma contiene numerose altre norme che, innanzitutto, disciplinano l'uso delle nuove tecnologie per le Forze di polizia (Titolo I, artt. 1-10), compreso il discusso ricorso ai dati biometrici ed al riconoscimento facciale, nonché l'incentivazione e la disciplina della ricerca anche sperimentale in questi ambiti; in secondo luogo, le norme delegate (Titolo II, artt. 11-20) introducono nuove disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiale, oltre a disposizioni processuali civili in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi. Per l'ambito del diritto penale sostanziale, il decreto – in conformità alla delega contenuta nella lettera b) del comma 5 dell'art. 24 l. 132/2025 – introduce un nuovo art. 437-*bis* c.p., collocato fra i delitti contro l'incolumità pubblica mediante violenza (Titolo VI, capo I del Libro II del codice penale), rubricato “omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale ed alterazione illecita di tali sistemi”, che contiene più fattispecie. La prima, di natura omissiva, sanziona, con la reclusione da uno a cinque anni, chi non adotta “le misure tecniche di sicurezza, previste per la progettazione, l'addestramento, la produzione, l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi ovvero omette di adottare misure di sorveglianza umana”, sempre che dall'omissione “derivi pericolo per la vita o l'incolumità pubblica o individuale”. Si tratta di un delitto doloso di pericolo concreto, rispetto a cui però non è chiaramente definito l'ambito degli obblighi di sicurezza o delle misure di sorveglianza umana la cui violazione costituisce reato.

Ai sensi del comma terzo, il fatto è punibile – con pena ridotta “da un terzo a un sesto” – anche a titolo di “colpa grave”, senza che parimenti siano allo stato chiaramente individuabili le regole cautelari cui le predette attività (in sé certamente lecite, ed anzi incentivate dallo stesso legislatore) devono però attenersi.

L'altra fattispecie delittuosa, prevista dal secondo comma, punibile solo a titolo di dolo, ma per vero non oggetto espresso della delega legislativa, consiste nella “alterazione” di detti sistemi d'intelligenza artificiale “ad alto rischio”, sempre che ne derivi pericolo concreto per i menzionati beni. Se invece dal fatto deriva “un pericolo per la sicurezza dello Stato” per tutti i menzionati delitti le pene sono più gravi.

Infine, l'ultimo comma punisce “l'utilizzatore professionale” di tali sistemi, che “intenzionalmente” (dunque con il grado più intenso del dolo, escluso quello eventuale o anche solo diretto) “omette...di adottare misure di sorveglianza umana”, sempre che “da tale omissione derivi, rispettivamente, pericolo per la vita o l'incolumità pubblica o individuale oppure un pericolo per la sicurezza dello Stato”.

Ne emerge senz'altro un apprezzabile rafforzamento della tutela della c.d. prospettiva antropocentrica e di responsabilizzazione per i rischi che possono derivare dai sistemi di intelligenza artificiale, cui si ispira la legge 132/2025 e lo stesso *AI Act*. Ma la formulazione delle fattispecie dà adito a molte perplessità sotto il profilo della determinatezza e dello stesso rispetto della riserva di legge in materia penale. Come perplessità nascono anche dal fatto che non è stata esercitata anche la delega prevista dalla lettera c) del menzionato art. 24 comma 5 l. 132/2025, secondo cui avrebbero dovuto essere precisati “i criteri di imputazione della responsabilità penale delle persone fisiche e amministrativa degli enti per gli illeciti inerenti a sistemi di intelligenza artificiale, che tenga conto del livello effettivo di controllo dei sistemi predetti da parte dell'agente”.

La mancanza di tale “precisazione” rileva anche perché il d.lgs. 160/2025 estende nel contempo l'ambito dei reati presupposto della responsabilità da reato delle persone giuridiche e degli enti, ai sensi del d.lgs. 8 giugno 2001, n. 231, nel quale viene inserito, dopo l'art. 25-*undecies*, l'art. 25-*vicies*, rubricato “Reati commessi con l'uso di sistemi di intelligenza artificiale” che prevede la sanzione pecuniaria da seicento a mille quote in relazione al delitto (in realtà: ai delitti) di cui al citato art. 437-*bis* c.p., e quella da duecento a settecento quote, in relazione al delitto di cui all'art. 612-*quater* (già introdotto dall'art. 1. 132/2025, che punisce l'illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale: c.d. *deep fake*), oltre – in entrambi i casi – alle sanzioni interdittive previste dall'art. 9, comma 2, lettere b), c), d) ed e) dello stesso d.lgs. 231/2001.

Dunque, un tassello importante per la tutela penale di beni giuridici fondamentali, che possono essere esposti a rischio dalla diffusione ed utilizzazione di sistemi di intelligenza artificiale, tuttavia criticabile per le tecniche

di formulazione utilizzate e, soprattutto, la mancanza di un approccio sistematico più ampio ai nuovi profili della responsabilità penale in questo campo (**L.P.**)

Il testo del decreto legislativo è consultabile al seguente [link](#).

2. Prove elettroniche nei procedimenti penali: i decreti legislativi attuativi del pacchetto europeo sugli ordini di conservazione e produzione

Con i decreti legislativi 30 dicembre 2025, nn. 215 e 216 (in G.U. n. 11 del 15 gennaio 2026, in vigore dal 30 gennaio 2026), l'Italia ha dato attuazione al pacchetto europeo sull'*e-evidence*, costituito dal regolamento (UE) 2023/1543, contenente disposizioni per l'introduzione degli ordini europei di conservazione e di acquisizione delle prove elettroniche e dalla direttiva (UE) 2023/1544 del 12 luglio 2023, che contiene disposizioni relative all'obbligatoria designazione di "stabilimenti designati" e nomina di "rappresentanti legali" negli Stati membri dell'Unione, da parte dei prestatori di servizi tenuti a dare esecuzione ai predetti ordini.

La prima esigenza è di rafforzare e sviluppare quell'unico "spazio di libertà, sicurezza e giustizia" rappresentato dall'Unione Europea, con un intervento incisivo nel campo giuridico e giudiziario, in particolare del diritto penale e del contrasto alla criminalità, da perseguire mediante la cooperazione giudiziaria e di polizia fra gli Stati membri e l'armonizzazione legislativa guidata dall'Unione.

Dall'altro lato, si persegue anche un'impellente esigenza del mercato digitalizzato: quella di garantire ai prestatori di servizi della società dell'informazione, che hanno e sono destinati ad avere un ruolo preponderante e sempre più importante nel prossimo sviluppo dell'economia e dell'integrazione sociale e politica dell'Unione, un quadro di disciplina uniforme in tutto il suo territorio, superando l'attuale frammentazione determinata dalla grande diversità dei diritti nazionali sulla possibilità di acquisire prove elettroniche da tali soggetti, anche al di fuori dei confini nazionali.

Il d.lgs. n. 215/2025, che adotta le misure organizzative e procedurali che il regolamento stesso demanda agli Stati membri per la sua concreta operatività, individua le Autorità competenti per la procedura di emissione degli ordini nel Pubblico Ministero e nel Giudice competente a pronunciarsi sulla richiesta. In caso di "emergenza" l'ordine può essere emesso anche da ufficiali di Polizia Giudiziaria con successiva convalida in termini tassativi, ma solo per acquisire i dati relativi all'abbonato (art. 2 d.lgs. 215 del 2025). In concreto, sia l'ordine europeo di produzione, sia l'ordine europeo di conservazione, non sono emessi da un'autorità od istituzione europea, ma dalle diverse autorità giudiziarie degli Stati membri "richiedenti" e vengono però ora diretti e trasmessi, non tramite le competenti autorità giudiziarie degli Stati membri "richiesti", bensì direttamente ai prestatori di servizi, che ne sono destinatari, tramite certificati denominati rispettivamente EPOC (certificato di ordine europeo di produzione) ed EPOC-PR (certificato di ordine europeo di conservazione), redatti secondo modelli standardizzati.

Il d.lgs. n. 216/2025 attua parallelamente la direttiva, imponendo ai prestatori di servizi digitali operanti nel mercato UE l'obbligo di designare un rappresentante legale ai fini della ricezione e dell'esecuzione degli ordini europei. Il nuovo assetto normativo, superando il tradizionale modello di cooperazione Stato-Stato, introduce un canale di interlocuzione diretta tra autorità giudiziaria e fornitori di servizi digitali nel territorio dell'Unione Europea, applicabile indipendentemente dalla loro sede legale, oltretutto ai prestatori di servizi digitali extraeuropei con un numero significativo di utenti negli Stati membri, al fine di assicurare tempi certi nell'acquisizione della prova digitale e di contrastarne la volatilità. In caso di violazione degli obblighi imposti dalle disposizioni applicabili alla ricezione, ottemperanza ed esecuzione delle decisioni e degli ordini in questione, il d.lgs. 216/2025 stabilisce una responsabilità in solito dei prestatori di servizi, degli stabilimenti da essi designati e dei rappresentanti legali degli stessi. (**Li.Pe**)

Il testo dei decreti legislativi 30 dicembre 2025, n. 215 e 216 è disponibile al seguente [link](#).

1. **Raccolta di dati biometrici dalla P.G.: la Corte di Giustizia UE l'ammette solo se strettamente necessaria**

Con la sentenza del 19 marzo 2026, emessa nella causa C-371/24, la Quinta Sezione della Corte di Giustizia dell'Unione Europea chiamata ad interpretare l'art. 10 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, ritiene illegittima una normativa interna che consenta alla Polizia Giudiziaria una raccolta investigativa sistematica, indifferenziata e generalizzata – quindi immotivata alle peculiarità del caso di specie – di dati biometrici (rilievi dattiloscopici e fotografie segnaletiche) di qualsiasi persona, anche solo sospettata di aver commesso, o tentato di commettere, un reato.

La legittimità della raccolta può essere compatibile con la normativa dell'Unione, infatti, solo qualora sussistano due condizioni imprescindibili a tutela dei diritti fondamentali: da un lato i) una normativa nazionale che definisca gli obiettivi e le finalità reali che giustifichino tale raccolta; dall'altro, ii) una singolare e specifica valutazione della necessità, nel singolo caso concreto, di procedere con la raccolta dei dati per realizzare tali obiettivi e finalità.

La Corte ricorda che i dati biometrici rientrano nella categoria dei dati personali c.d. "sensibili", per cui è imposta una loro tutela rafforzata: la legittimità della normativa interna impone, pertanto, la presenza simultanea di due requisiti: una disciplina chiara a livello interno, posta a tutela dei diritti fondamentali, che individui le finalità e gli obiettivi del loro trattamento, a cui si affianchi un obbligo di concreta motivazione nel singolo caso di specie sul carattere "strettamente necessario" della loro raccolta. (S.T.).

[Corte di Giustizia dell'Unione Europea, sentenza del 19 marzo 2026, Causa C-371/24.](#)

2. **Corte Costituzionale: impugnazione depositata ad indirizzo errato ed interpretazione costituzionalmente conforme**

Nel solco della precedente pronuncia, con la sentenza n. 77 del 14 maggio 2026, la Consulta ha dichiarato non fondate le questioni di legittimità costituzionale sollevate da due ordinanze della Prima Sezione Penale della Corte di cassazione dell'art. 87-bis, commi 7, lett. c), e 8, del d.lgs. n. 150 del 2022 in riferimento agli artt. 3 e 24 della Costituzione, nonché in relazione all'art. 6, paragrafo 1, della Convenzione europea dei diritti dell'uomo: *«nella parte in cui sancisce l'inammissibilità dell'impugnazione trasmessa ad indirizzo di posta elettronica certificata diverso da quello prescritto (costituito dall'indirizzo assegnato all'ufficio che ha emesso il provvedimento impugnato) pur quando essa pervenga al giudice a quo entro il termine perentorio di proposizione»*.

In entrambi i casi, i ricorrenti nei giudizi *a quibus* avevano presentato i propri atti di impugnazione di un provvedimento del Magistrato di Sorveglianza, ad indirizzi PEC riferibili al Tribunale di Sorveglianza, con la conseguente pronuncia di loro inammissibilità. Infatti, costoro non avevano osservato le disposizioni di cui al censurato art. 87-bis, comma 7, lettera c), del d.lgs. n. 150 del 2022, nella parte in cui stabilisce che l'impugnazione è inammissibile *«quando l'atto è trasmesso a un indirizzo di posta elettronica certificata non riferibile [...] all'ufficio che ha emesso il provvedimento impugnato»*, e dunque anche quando esso sia riferibile all'ufficio competente per il giudizio sull'impugnazione. Nei due casi oggetto dei procedimenti *a quibus*, peraltro, la cancelleria del Tribunale aveva trasmesso analogicamente, quindi in forma cartacea, gli atti di impugnazione all'Ufficio di sorveglianza competente alla ricezione dell'impugnazione, prima della scadenza del termine previsto per l'impugnazione. Pertanto, osservavano le Corti rimettenti, l'errore sarebbe stato "sanato" e sarebbe rimasto "privo di conseguenze effettive".

La disciplina dell'art. 87-bis, commi 7, lett. c), e 8, d.lgs. n. 150/2022 è costituzionalmente compatibile, a condizione che sia interpretata nel senso che *“l'inammissibilità resta esclusa nell'ipotesi in cui l'atto di impugnazione sia stato inoltrato, su iniziativa della cancelleria cui è riferibile l'indirizzo PEC cui esso sia stato erroneamente presentato, all'indirizzo PEC – anch'esso incluso nell'elenco del DGSIA – riferito all'ufficio del giudice che ha emesso il provvedimento, laddove l'inoltro sia effettuato entro il termine*

perentorio stabilito per l'impugnazione medesima". In tal caso, la "*continuità digitale*" del flusso telematico e il tempestivo raggiungimento dello scopo impongono di escludere la sanzione di inammissibilità, in ossequio a un'interpretazione costituzionalmente e convenzionalmente orientata (**S.T.**).

[Corte cost., Sentenza, 14/05/2026, n. 77.](#)

3. Corte di Giustizia: il diritto europeo non osta al sequestro di messaggi di posta elettronica professionali scambiati tra i dipendenti e gli amministratori delle imprese oggetto di un'indagine

La Grande Sezione della Corte di Giustizia, con sentenza del 16.7.2026, emessa nelle cause riunite C-258/23, C-259/23 e C-260/23, ha stabilito che nell'ambito di un'indagine avente ad oggetto la presunta violazione delle norme in materia di concorrenza, l'Autorità nazionale Garante della Concorrenza può disporre il sequestro dei messaggi di posta elettronica scambiati nei locali professionali o commerciali tra i dipendenti e gli amministratori delle società sottoposte ad indagine senza che ciò comporti una violazione del diritto dell'Unione.

La Corte riconosce che il sequestro di messaggi di posta elettronica di carattere professionale costituisca una limitazione al diritto al rispetto della vita privata e familiare e al diritto alla protezione dei dati di carattere personale; tuttavia, tali limitazioni sono giustificate dalla finalità di preservare una concorrenza leale, quale finalità di interesse generale riconosciuta dall'Unione europea.

Tali limitazioni, precisa la Corte, sono ammesse anche in assenza di un'autorizzazione preventiva rilasciata da un giudice poiché normalmente, la tutela degli individui contro gli abusi e gli arbitri delle Autorità competenti è garantita da discipline normative che prevedono un successivo controllo giurisdizionale completo.

Nel caso in cui, invece, il sequestro dei messaggi di posta elettronica sia effettuato su dispositivi utilizzati anche per finalità private e non solo lavorative, è necessaria l'autorizzazione preventiva di un giudice o di un organo amministrativo indipendente poiché l'accesso a tali dati potrebbe consentire l'ottenimento di informazioni sulla vita privata degli interessati, integrando una grave ingerenza nei diritti fondamentali sopra richiamati (**Li.Pe.** e **B.P.**).

[Corte di Giustizia dell'Unione Europea, sentenza del 16 luglio 2026, cause riunite C-258/23, C-259/23 e C-260/23](#)

4. Sezioni Unite: impugnazione inammissibile se la PEC non rientra nell'elenco ufficiale DGSIA

La Cassazione aderisce alla linea del rigore metodologico e procedurale: inammissibile l'atto d'impugnazione inviato ad un indirizzo PEC non ricompreso nell'elenco ufficiale del decreto direttoriale del DGSIA del 9 novembre 2020, quand'anche riferibile all'ufficio del destinatario corretto.

Il deposito telematico, infatti, è disciplinato in modo analitico, con regole tassative e causa di inammissibilità tipizzate ed inderogabili, che escludono interpretazioni correttive fondate sul raggiungimento dello scopo. Inoltre, non può ritenersi scusabile l'errore commesso dal difensore nell'individuazione dell'indirizzo telematico corretto, dato che il provvedimento ministeriale sopra indicato è atto pubblico, facilmente accessibile, individuabile nelle forme chiaramente riconosciute e riconoscibili, quali "*depositoattipenali*", seguite dalla specificazione dell'ufficio competente.

Aderendo a quest'impostazione, la Corte esclude un'interpretazione estensiva o flessibile del sistema, con la conseguenza di non poter ammettere il deposito telematico presso qualsiasi indirizzo riferibile all'ufficio giudiziario, compresi quelli non istituzionalmente deputati alla ricezione degli atti. Una tale interpretazione, infatti, si sostanzierebbe nell'annullamento di ogni requisito di forma, ponendosi in contrasto con la *ratio legis* e con il principio di legalità processuale. Ciò, parimenti, nell'ipotesi in cui l'atto inoltrato ad indirizzo PEC errato, venga analogicamente trasmesso dal relativo funzionario all'ufficio competente all'elaborazione dell'impugnazione.

A conclusione difforme, invece, perviene la Corte nell'ipotesi in cui l'atto d'impugnazione, inizialmente veicolato telematicamente ad indirizzo PEC non contemplato nel decreto DGSIA – seppur riferibile all'organo giudiziario competente – venga inoltrato telematicamente dal cancelliere, addetto a quell'ufficio, all'indirizzo abilitato alla ricezione dell'atto d'impugnazione, entro il termine decadenziale previsto dalla legge. Infatti, la trasmissione interna tra caselle PEC dello stesso ufficio giudiziario garantisce il rispetto dell'*iter* telematico

imposto *ex lege*. Così facendo, l'interpretazione garantisce al contempo il diritto all'impugnazione, sottoposta così tempestivamente al giudice competente con modalità conformi al sistema, e la "continuità digitale" così assicurata dall'inoltro del cancelliere, sebbene non obbligato giuridicamente a quest'operazione. Solo in questi termini, la fattispecie rientra nella lettera della norma e consente di rispettare gli obblighi di informatizzazione gravanti sulla professione (**S.T.**).

[Cass., Sez. Unite pen., Sent., \(data ud. 11/12/2025\) 18/02/2026, n. 6565.](#)

5. Truffa mediante l'utilizzo di carte di credito

Integra il reato di truffa, e non di insolvenza fraudolenta, la condotta del reo che usufruisce gratuitamente di un soggiorno presso una struttura alberghiera, fornendo per i pagamenti gli estremi di carte di credito di terzi ignari, pagamenti successivamente non andati a buon fine per la revoca delle transazioni per effetto del disconoscimento da parte dei titolari delle carte, in quanto sussistono sia l'induzione in errore dell'albergatore sulla effettività delle operazioni e l'ingiusto profitto consistente nella fruizione del soggiorno, mentre non sussiste la dissimulazione dello stato di insolvenza. (**C.C.**)

[Cass. pen., sez. II, ud. 9 settembre 2026 \(dep. 11 settembre 2026\), n. 33382](#)

6. Luogo di consumazione del reato di truffa online

Nel caso della truffa, la percezione dell'ingiusto profitto costituisce prova e non mero indizio della riferibilità all'agente della condotta costitutiva la fattispecie illecita, poiché la truffa contrattuale realizzata attraverso la vendita di beni "on line" in cui il pagamento eseguito dalla parte offesa avvenga tramite bonifico bancario con accredito su conto corrente, si consuma nel luogo ove l'agente consegue l'ingiusto profitto tramite la riscossione della somma e non già in quello in cui viene data la disposizione per il pagamento da parte della persona offesa. Pertanto, il percettore del profitto illecito, individuato nel caso di specie in modo puntuale, con riferimento all'evidente disponibilità e titolarità della carta Postepay, pone in essere una frazione essenziale della condotta tipica e vi è quindi dimostrazione del suo ruolo essenziale nella consumazione dell'illecito. (**C.C.**)

[Cass. pen., sez. II, ud. 19 giugno 2026 \(dep. 3 luglio 2026\), n. 25160](#)

7. La c.d. "allucinazione informatica" e l'utilizzo di strumenti di I.A. generativa

Con la presente ordinanza la Corte di Cassazione ha avuto modo di rilevare in via preliminare come i richiami giurisprudenziali contenuti nel ricorso non si attagliassero al caso concreto, essendo frutto della c.d. allucinazione informatica, conseguente all'utilizzo di strumenti di AI generativa. (**S.D.**)

[Cass. pen., Sez. VII, Ord., \(data ud. 27/02/2026\) 26/03/2026, n. 11431](#)

In tema di intelligenza artificiale, la Corte di Cassazione ha precisato come la citazione di precedenti giurisprudenziali alterati o inesistenti, frutto, pertanto, di c.d. "allucinazione informatica", rappresenti un chiaro segno di trascuratezza professionale e costituisca "un indice particolarmente significativo di colpa qualificata nelle determinazioni della causa di inammissibilità", giustificando, di conseguenza, l'irrogazione della più elevata sanzione di cui all'art. 616 c.p.p. (**S.D.**)

[Cass. pen., Sez. III, Sent., \(data ud. 11/06/2026\) 22/06/2026, n. 23006](#)

8. Frode informatica aggravata dal furto d'identità digitale

La Cassazione è tornata a pronunciarsi sulla frode informatica aggravata, ex art. 640-ter, comma terzo, c.p., dal furto di identità digitale, ritenendola sussistente nella condotta di chi accede abusivamente al sistema

operativo di un servizio di *home banking* utilizzando le credenziali di accesso riconducibili all'identità digitale della persona offesa. Per la Corte ciò che risulta determinante ai fini della ricorrenza dell'ipotesi aggravata non è tanto la modalità attraverso cui le credenziali di accesso siano state originariamente acquisite, quanto l'utilizzazione consapevole delle stesse per realizzare un'interferenza non autorizzata nel sistema informatico, produttiva di un vantaggio patrimoniale indebito con artificiosa rappresentazione dell'operazione come proveniente dal titolare del rapporto bancario. **(R.M.V.)**

[Cass. pen., Sez. II, Sent., \(data ud. 30/01/2026\) 24/04/2026, n. 14918](#)

9. La minorata difesa della truffa on line

Nel caso di truffa *on line* sussiste l'aggravante della minorata difesa solo quando l'autore abbia tratto, consapevolmente ed in concreto, specifici vantaggi dall'utilizzazione dello strumento della rete e specificamente dalle modalità telematiche della vendita. A tal fine per la Corte la circostanza che il primo contatto tra gli inserzionisti di annunci, persone offese del reato, e l'imputato sia avvenuto *online* non è sufficiente in presenza di successive trattative che sono state condotte telefonicamente. **(R.M.V.)**

[Cass. pen., Sez. II, Sent., \(data ud. 26/03/2026\) 26/05/2026, n. 18913](#)

10. Smart card pirata e concorso nei reati informatici prodromici

La rivendita di codici di accesso a sistemi abusivi e *smart card* pirata ad utenti privati per fine di lucro costituisce la parte finale di un'azione criminosa complessiva finalizzata a truffare le piattaforme a pagamento, cosicché sussiste concorso dei rivenditori di tali strumenti anche nella commissione da parte di terzi sia della condotta di accesso abusivo a sistema informatico, sia di quella di truffa informatica data la loro conoscenza delle attività dei correi nelle fasi antecedenti.

Per la corte la predetta rivendita integra, altresì, delitto di cui all'art. 171-ter della legge n. [633/1941](#) in quanto comportante l'abusiva trasmissione di opere dell'ingegno coperte dal diritto d'autore senza alcuna autorizzazione del titolare. **(R.M.V.)**

[Cass. pen., Sez. II, Sent., \(data ud. 06/03/2026\) 18/03/2026, n. 10451](#)

11. Pornografia minorile mediante programmi di file-sharing

La Cassazione ribadisce che l'utilizzo di programmi di *file sharing* (come *eMule*) non integra automaticamente il reato di diffusione di materiale pedopornografico, ma è necessario accertare ulteriori elementi che dimostrino la volontà, anche solo eventuale, di divulgare i file. Nel caso concreto, la condivisione durante il *download* con altri utenti della rete e fruitori del programma, la piena conoscenza del funzionamento del programma e l'ingente quantità di contenuti pedopornografici rinvenuti nei dispositivi dell'imputato consentono di ritenere ai fini cautelari sussistente oltre che il delitto di detenzione, anche quello di diffusione consapevole del materiale pedopornografico. **(R.M.V.)**

[Cass. pen., Sez. III, Sent., \(data ud. 09/12/2025\) 11/02/2026, n. 5443](#)

12. Quando un commento pubblicato sui social integra il delitto di diffamazione

In contrasto con quanto deciso in primo grado dal Tribunale di Piacenza, la Sezione quinta della Suprema Corte di Cassazione ha specificato come un contenuto pubblicato su *Facebook* non debba essere ritenuto diffamatorio qualora si evinca il carattere ironico e colloquiale dello stesso.

Il Giudice delle leggi ha infatti ribadito un consolidato orientamento giurisprudenziale, per cui “*ai fini della configurabilità del delitto di diffamazione, è necessario che le parole utilizzate siano attributive di qualità sfavorevoli alla persona offesa, ovvero, che gettino, comunque, una luce negativa su quest'ultima*” (cfr. da

ultimo, Cass. Pen. Sez. V, 09.04.2024, n. 21869), precisando, inoltre, che detta affermazione dispregiativa debba essere avvertita e percepita come tale dal c.d. “soggetto medio”. **(S.D.)**

[Cass. pen., Sez. V, Sent., \(data ud. 18/03/2026\) 12/05/2026, n. 17017](#)

13. Sequestro probatorio e diritto alla privacy

La Corte di legittimità ha recentemente ribadito un principio consolidato in giurisprudenza, secondo il quale il sequestro probatorio di dispositivi elettronici ed, in particolare, di *smartphone*, richiede una motivazione “*specificata e non meramente generica*” precisando, infatti, come il Pubblico Ministero non possa acquisire, tramite tale mezzo di ricerca della prova, tutti i messaggi, le fotografie e gli altri documenti privati contenuti nello *smartphone* dell’indagato, “*senza indicare le ragioni per le quali, ai fini dell’accertamento dei reati ipotizzati, si rende imprescindibile la integrale verifica di tutti i predetti dati*”, sacrificando, di conseguenza, il diritto di quest’ultimo alla segretezza della corrispondenza. **(S.D.)**

[Cass. pen., Sez. II, Sent., \(data ud. 23/04/2026\) 07/05/2026, n. 16495](#)

14. Violenza sessuale “a distanza”

Con la sentenza n. 16564/2026 Reg. Gen. Sent., la terza sezione della Suprema Corte di Cassazione ha avuto modo di esprimersi in tema di pedopornografia (art. 600-ter c.p.), violenza sessuale (art. 609-bis c.p.) ed atti sessuali con minorenni (art. 609-quater c.p.), evidenziando, anzitutto, come sia il reato di cui all’art. 609-bis c.p. sia quello disciplinato dall’art. 609-quater c.p. possano essere commessi anche “fra assenti”, non essendo necessaria la contestuale presenza fisica dei soggetti.

Nello specifico si è precisato come il delitto di violenza sessuale possa dirsi integrato solo qualora la condotta minatoria o quella di abuso di autorità “*abbiano una forza tale da perdurare nel tempo*”, mentre per quanto concerne l’art. 609-quater c.p. “*è sufficiente che vi sia un mero rapporto di mera causalità fra la condotta del soggetto agente e quella della persona offesa*”.

La Corte di legittimità ha, poi, avuto modo di soffermarsi su ulteriori aspetti rilevanti, tra i quali rientra senz’altro il concetto di “utilizzo” del minore, già oggetto di numerosi interventi interpretativi (cfr. *ex multis* Cass. Pen. Sez. III, Sent. 21.11.2024, n. 5700), specificando come tale requisito, previsto espressamente dall’art. 600-ter c.p., debba essere rilevato ogni volta che il minore diventa oggetto di una certa condotta e non un soggetto autonomo in grado di esprimere un consenso libero e non viziato dall’adulto. **(S.D.)**

[Cass. pen., Sez. III, Sent., \(data ud. 19/11/2025\) 08/05/2026, n. 16564](#)

15. Diffamazione a mezzo “Facebook”: limiti della prova liberatoria

Con la sentenza in esame, la Quinta Sezione Penale della Corte di Cassazione ha deciso l’impugnativa proposta dal ricorrente in tema di diffamazione aggravata dal mezzo informatico, *ex art. 595*, commi 1 e 3, c.p., per aver costui pubblicato sul social network “*Facebook*” messaggi e post lesivi dell’onore e della reputazione professionale di due agenti assicurativi, in particolare, affermando l’appropriazione, da parte di costoro, di somme di denaro al proprio anziano genitore.

In sede di legittimità, l’imputato si era difeso rappresentando l’omessa valutazione, e quindi il mancato riconoscimento, della sussistenza degli estremi della prova liberatoria, quale causa di esclusione della punibilità, che lo avrebbe mandato proscioltto. Egli, infatti, nel merito aveva allegato la circostanza che le Persone offese dalla presunta diffamazione fossero soggette a procedimento penale per i medesimi fatti da lui indicati nei post sopra indicati.

La Corte, ponendosi in continuità con l’insegnamento consolidato, nel rigettare il ricorso ha ricordato come non sia sufficiente che nei confronti della persona la cui reputazione è stata offesa, sia pendente un procedimento penale. Questa circostanza, infatti, rappresenta solo la condizione di fatto che abilita l’ingresso della prova liberatoria nel processo a carico del presunto diffamante. L’onere della prova, che grava su costui,

potrà ritenersi assolto sia in forma diretta, con la piena dimostrazione dell'esistenza della circostanza attribuita all'interno del procedimento stesso, sia in forma indiretta, acquisendo la pronuncia irrevocabile di condanna. Pertanto, l'esclusione della punibilità dell'imputato si fonda non tanto sulla mera allegazione della sussistenza del procedimento penale a carico della persona offesa, quanto piuttosto sull'elemento oggettivo della verità del fatto oggetto della presunta diffamazione, la cui prova grava inevitabilmente sulla difesa (*S.T.*).

[Cass., Sez. V pen., Sent., \(data ud. 05/11/2025\) 02/02/2026, n. 4263.](#)

16. Minaccia nell'estorsione: configurabile in presenza di messaggi intimidatori inviati su WhatsApp

La Seconda Sezione Penale della Corte Suprema ribadisce come l'invio di messaggi *WhatsApp* alla persona offesa dal reato, contenenti espressioni larvate, indirette o allusive, possa integrare il concetto di minaccia penalmente rilevante, che connota la condotta del reato di estorsione, ai sensi dell'art. 629 c.p.. Tuttavia, l'invio minatorio non basta, dovendo inserirsi in un concreto contesto relazionale e temporale di successivi episodi violenti, idonei ad incutere oggettivamente timore agli occhi della stessa, incidendo così nella libertà di autodeterminazione della persona offesa (*S.T.*)

[Cass. pen., Sez. II, Sent., \(data ud. 30/04/2026\) 27/05/2026, n. 19338](#)

17. Responsabilità del blogger: è diffamazione aggravata se non rimuove i contenuti offensivi

Con la sentenza in commento, la Quinta Sezione Penale della Suprema Corte conferma la pronuncia di colpevolezza pronunciata per il delitto di diffamazione aggravata, ex art. 595, comma terzo, c.p., nei confronti del gestore di un *blog* che non provvede alla rimozione dei contenuti diffamatori ivi pubblicati da terzi.

In particolare, la Corte ha valorizzato la scelta del *blogger* di mantenere *online* i contenuti offensivi, nonostante il loro patente contenuto diffamatorio, estrinsecando così una condotta equivalente a quella volta alla consapevole condivisione del contenuto lesivo dell'altrui reputazione, di cui ha parimenti consentito – ed anzi ampliato – la diffusione in rete.

Per ricondurre tale scelta ad una “consapevole condivisione” di questi contenuti, i Giudici di merito hanno valorizzato: i) la continuità del *blog* con il periodico cartaceo che l'imputato dirigeva e di cui era proprietario; ii) l'utilizzo in tutti gli undici articoli diffamatori, del medesimo segno identificativo dell'Associazione di cui l'imputato era Presidente; nonché iii) la condivisione dei contenuti degli articoli sui profili *social* dell'imputato, con invito alla lettura dei post sul *blog*. Di qui la conferma della pronuncia della Corte di Venezia, il rigetto del ricorso e la condanna dell'imputato al pagamento delle spese processuali (*S.T.*).

[Cass. pen. Sez. V. Sent. \(data ud. 25/03/2026\) 17/07/2026, n. 27079](#)

NOVITÀ RILEVANTI A LIVELLO NAZIONALE

1. Mediaset contro l'IA: la prima causa in Italia avverso un sistema di intelligenza artificiale

Con atto di citazione depositato lo scorso dicembre, *Mediaset* ha dato il via alla prima causa in Italia avverso un sistema di intelligenza artificiale.

Nello specifico, la società milanese ha agito contro *Perplexity A.I.*, denunciando la violazione del c.d. diritto di *opt-out*, previsto espressamente dall'art. 4 della Direttiva Copyright (Direttiva UE 2019/790), che consente di opporsi alla possibilità che proprie opere siano destinate all'addestramento di sistemi di I.A.

Mediaset sostiene, infatti, che *Perplexity* si starebbe “addestrando” avvalendosi dei propri formati, malgrado la stessa società di Cologno Monzese combatta da tempo questo fenomeno, avendo, infatti, introdotto nelle proprie trasmissioni il monito: “*E' severamente vietato ogni utilizzo delle immagini trasmesse atto all'addestramento di sistemi di IA generativa così come l'utilizzo di mezzi automatizzati di data scraping*”.

Nell'attesa che il giudice civile si pronunci, vale la pena, dunque, di sottolineare l'attualità di questo procedimento, nella convinzione che non rimarrà un caso isolato, ma verrà presto seguito da altri contenziosi concernenti la medesima *causa petendi*. (*S.D.*)

Il comunicato stampa di Mediaset consultabile al seguente [link](#).

2. L'introduzione dello Sportello Unico Nazionale dei dati protetti

In attuazione di quanto disposto dall'art. 8 del Regolamento (UE) 2022/868 (*Data Governance Act*), dal 28 maggio 2026 è stato reso operativo in Italia lo Sportello Unico Nazionale dei Dati protetti, con l'intento di favorire la trasparenza e, in particolare, l'accesso da parte dei cittadini interessati ai c.d. dati informatici protetti, come i dati sanitari e quelli salvaguardati dal diritto di proprietà intellettuale, i quali, infatti, non sono liberamente accessibili da chiunque.

La nascita di questo sportello rappresenta una decisiva svolta, che comporterà, come conseguenza, il sorgere di nuovi obblighi in capo alla Pubblica Amministrazione, la quale sarà infatti chiamata ad annotare tutti i dati protetti.

Tale sportello garantirà dunque una maggiore tutela del cittadino, inserendosi in un panorama ben più vasto, volto a consentire la più ampia circolazione di dati ed a favorire la collaborazione tra la Pubblica Amministrazione ed il cittadino stesso **(S.D.)**

Il comunicato dell'Agenzia per l'Italia Digitale è disponibile al seguente [link](#).

3. Accesso alle e-mail aziendali da parte di un ex-dipendente: il sì del Garante privacy

Il Garante della protezione dei dati personali si è recentemente espresso su un caso di particolare rilevanza, concernente la possibilità, in capo all'ex dipendente, di accedere alla propria casella di posta elettronica aziendale, malgrado la cessazione del rapporto lavorativo, in quanto la società aveva consentito l'accesso limitatamente ai soli dati personali.

Il Garante ha dunque ritenuto che tale decisione non fosse legittima, poiché in contrasto con quanto disposto dagli artt. 12 e 15 del regolamento UE 2016/679 (GDPR), dato che lo scambio di corrispondenza, seppur intrattenuto sull'*account* aziendale, non è di "piena ed esclusiva disponibilità dell'azienda stessa". **(S.D.)**

Il provvedimento del Garante della Privacy del 12.3.2026, n. 165 è consultabile al seguente [link](#).

4. Dossier Viminale di agosto 2026: il quadro della sicurezza in Italia

Nel dossier pubblicato dal Ministro dell'Interno Piantedosi, utile ad avere un quadro dei numeri che caratterizzano la criminalità in Italia, per quanto di nostro interesse, una sezione è dedicata all'approfondimento della "*Sicurezza informatica e cibernetica*".

L'analisi di campione è stata effettuata nel periodo 1° gennaio – 30 giugno 2025 e 1° gennaio – 30 giugno 2026.

I numeri riportati parlano di una riduzione del 16,9 % degli attacchi rilevati a danno delle infrastrutture critiche (reti energetiche, ospedali, infrastruttura di trasporto, etc.): 4.911 contro i 4.082 del primo semestre dell'anno in corso. Quanto al cyberterrorismo, si segnala anche in questo caso una riduzione del 23,3 % dei casi, passando da 116 a 89. Rispetto al primo semestre del 2025, invece, aumentano gli indagati del 71% per i reati connessi **(S.T.)**.

Il dossier completo è rinvenibile al seguente [link](#).

VOLUMI E CONTRIBUTI DOTTRINALI DI RILIEVO

Altalex

Riccio G. M., *Grok, deepfake e immagini sessualizzanti: quali rimedi in Europa e negli Stati Uniti*, 19.3.2026.

Biarella L., *L'UE verso la sovranità tecnologica, nuovo pacchetto per indipendenza e innovazione*, 5.6.2026.

Romito C. C., *AI Act e attuazione italiana: il primato normativo alla prova della tenuta del sistema*, 16.06.2026.

Diritto di Internet

Picotti L., Gli ordini di produzione e conservazione di prove elettroniche nei procedimenti penali e l'implementazione in Italia della normativa dell'Unione, n. 3/2026, .

Giurisprudenza penale

La nuova Direttiva sulla lotta contro la corruzione approvata dal Parlamento europeo, 27.3.2026.

Rinaldini F., Intelligenza artificiale: in arrivo nuovi reati e nuove responsabilità per gli enti, 02.09.2026.

Sistema Penale

Picotti L., I contenuti penali della legge sull'intelligenza artificiale, 2.12.2025

De Lazzaro C., L'acquisizione delle prove elettroniche nello spazio di libertà, sicurezza e giustizia: una prima implementazione dell'*e-evidence package*, 2.2.2026

Intelligenza artificiale: una prima pronuncia di inammissibilità di un ricorso per cassazione imputabile (anche) a richiami giurisprudenziali non pertinenti, 20.5.2026

Fragasso B., Disposizioni attuative in materia di intelligenza artificiale: il reato di omessa adozione di misure di sicurezza nei sistemi di I.A. e altre novità in materia di autorità di vigilanza, identificazione biometrica, responsabilità da reato degli enti e responsabilità civile, 12.6.2026.

Parodi C., Le nuove Raccomandazioni del CSM sull'intelligenza artificiale nella giustizia. Dalla cautela difensiva alla governance del rischio, 24.7.2026

Salvi G., La giurisdizione penale e l'intelligenza artificiale: meriti e limiti della scelta regolatoria e classificatoria dell'Unione europea e prospettive di evoluzione del diritto nazionale, 4.08.2026.