CYBER- and AI- CRIME

Rassegna delle novità (dicembre 2024 – aprile 2025)

Rassegna di novità in materia di diritto penale e nuove tecnologie

Responsabile scientifico: Prof. Lorenzo Picotti - monitoraggio a cura di Alice Baccin, Chiara Crescioli, Beatrice Panattoni, Lisa Perobello, Simone Tarantino, Rosa Maria Vadalà; redazione a cura di Lorenzo Picotti, Rosa Maria Vadalà, Chiara Crescioli, Simone Tarantino e Lisa Perobello.

NOVITÀ SOVRANAZIONALI

1. La Convenzione Onu sulla criminalità informatica (Cybercrime Convention)

In data 24 dicembre 2024, l'Assemblea Generale delle Nazioni Unite ha adottato la Convenzione in oggetto, che mira a combattere la criminalità informatica in modo più efficiente, rafforzando la cooperazione internazionale e fornendo assistenza tecnica, in particolare, ai paesi in via di sviluppo. La Convenzione, che sarà prossimamente aperta alla firma dei singoli Stati, si compone di 8 capitoli, di cui i capitoli da II a V fissano gli obblighi di penalizzazione e le misure probatorie e processuali. Per quest'ultime è richiesto che debbano essere adottate per tutti i reati che sono commessi attraverso un sistema informatico o telematico e quando si tratta di raccogliere prove elettronicamente, e non solo per i reati previsti dalla Convenzione. Relativamente agli obblighi di penalizzazione, sono previsti 17 reati fra cui, specificamente, accanto ai reati informatici tradizionali, come l'accesso abusivo o la frode informatica, anche i reati di pornografia minorile e *grooming* mediante la rete, nonché quelli di diffusione non consentita di immagini intime e di riciclaggio. La Convenzione dedica particolare attenzione al contrasto della dimensione economica della criminalità informatica, prevedendo disposizioni specifiche sulla cooperazione internazionale finalizzata alla confisca e sulla possibilità di concludere accordi o intese bilaterali o multilaterali per istituire organismi investigativi comuni. Per tutti i reati previsti è altresì richiesto che gli Stati, tenendo conto della loro gravità ed in conformità alla relativa legislazione interna, fissino un ampio termine di prescrizione, stabilendone uno più lungo o disponendo la sospensione della prescrizione quando la persona, sospettata di aver commesso il reato, si sia sottratta all'amministrazione della giustizia (R.M.V.).

Il testo della convenzione è consultabile in inglese, francese e spagnolo al seguente link. Per primi commenti in italiano si rinvia alla sottostante bibliografia.

2. Il Rapporto congiunto Eurojust ed Europol su "Common Challenges in Cybercrime"

Il rapporto, pubblicato il 31 gennaio 2025, evidenzia la persistenza nell'anno 2024 di criticità nell'attività investigativa e di contrasto alla criminalità informatica, nonostante iniziative legislative anche recenti, come il *Cloud Act*, l'*AI Act* e il secondo protocollo addizionale della Convenzione di Budapest. Le criticità afferiscono, in particolare, alla gestione di grandi volumi di dati, alle sfide poste dai servizi di anonimizzazione e dalle tecnologie che oscurano le posizioni degli utenti, creando barriere sostanziali al tracciamento delle attività illecite ed ostacoli nella cooperazione internazionale.
Si sottolinea la necessità di soluzioni adattabili alla natura dinamica delle minacce informatiche e che consentano il potenziamento delle capacità tecniche e operative delle forze dell'ordine per tenere il passo con i progressi tecnologici e contrastare preventivamente le minacce emergenti. Inoltre, le crescenti sfide relative alla conservazione dei dati, alle barriere giurisdizionali e alle complicazioni insite nei partenariati pubblico-privati richiedono un approccio che bilanci in maniera equilibrata misure di sicurezza rigorose con la salvaguardia della *privacy* e delle libertà civili (R.M.V.).

Il testo del rapporto è disponibile al seguente link

3. Linee guida della Commissione europea sulle pratiche vietate in materia di intelligenza artificiale

In data 4 febbraio 2025, la Commissione europea ha adottato, conformemente all'art. 96 dell'*AI Act* ed in vista dell'applicabilità dei divieti già vigenti a partire dal 2 febbraio 2025, le linee Guida relative alle pratiche di intelligenza artificiale vietate dall'art. 5. Queste indicazioni mirano a garantire un'applicazione coerente, efficace e uniforme del regolamento, in ausilio a fornitori ed utilizzatori di sistemi di intelligenza artificiale. A tal fine, per ciascuna delle quattro categorie di AI vietate, vengono fornite chiarificazioni sul significato dei concetti identificativi e delineati esempi d'implementazioni vietate. Emerge in questo modo lo sforzo di fornire indicazioni concretamente attuabili perchè calate sulla specificità della funzione e dell'oggetto del singolo divieto e costruite per differenziare le pratiche illecite da quelle lecite.
Ad esempio, con specifico riferimento ai sistemi di intelligenza artificiale, che prevedono il rischio che una persona fisica commetta un reato, basandosi esclusivamente sulla profilazione o sulla valutazione dei tratti e delle caratteristiche della personalità, le prescrizioni date cercano di distinguerle chiaramente dai sistemi predettivi che sono, invece, ammessi ancorchè costituiscano sistemi di AI ad alto rischio.
Premesso che il divieto si applica indipendentemente dal fatto che il sistema AI profili o valuti i tratti e le caratteristiche della personalità di una sola persona fisica o di un gruppo di persone fisiche simultaneamente, la Commissione chiarisce che l'uso del termine "esclusivamente" comporta che è vietato il sistema che non considera altri elementi nella valutazione del rischio Questi altri elementi devono però essere costituiti da fatti oggettivi, significativi e rilevanti affinché sia possibile giustificare la conclusione che il divieto non si applica. Nel caso, invece, del divieto di sistemi di IA per creare *database* per riconoscimento facciale non è richiesto che l'unico scopo del *databse* sia quello di essere utilizzato per il riconoscimento facciale, bastando che possa essere per questo impiegabile. Allo stesso modo lo *scraping* indiscriminato di immagini facciali è ritenuto sussistente quando la raccolta di dati o contenuti avvenga senza un focus specifico su un singolo individuo o su un gruppo di individui, a prescindere dal rispetto dei protocolli di *opt-ou*t di internet, come robot.txt. Per la Commissione si è, però, comunque al cospetto di *scraping* vietato quando il risultato finale sia funzionalmente lo stesso di un'operazione di *scraping* indiscriminata fin dall'inizio. A fronte di ciò ed in generale per evitare impieghi che siano nei fatti elusivi dei divieti, si incoraggiano l'adozione di misure di trasparenza e *audit* dei sistemi IA per garantire in itinere il rispetto delle norme (R.M. V.)

Il testo delle linee guida è disponibile al seguente link

4. Report Europol "The changing DNA of serious and organised crime"

Il report, pubblicato nel mese di marzo 2025, evidenzia come il crimine organizzato grave attenti alla stabilità politica, economica e sociale attraverso il riciclaggio dei proventi illeciti, la perpetuazione della violenza, della corruzione e anche della presenza *online*. *Internet* rappresenta non solo uno strumento potente per occultare varie forme di attività criminale, ma anche il principale ecosistema per la commissione di determinati reati, come frodi informatiche o distribuzione di materiale pedopornografico. Le reti criminali coinvolte nel traffico di droga beneficiano delle infrastrutture digitali per comunicare o per ottenere fraudolentemente informazioni sensibili (attraverso intrusioni nei sistemi digitali o corruzione degli utenti) su spedizioni contenenti carichi di droga nascosti. Oltre a utilizzare applicazioni di mappatura e prenotazione online per organizzare gli spostamenti, le reti criminali promuovono sui *social media* servizi di traffico di migranti, richiedendo pagamenti in criptovaluta. L'uso di quest'ultime ha permesso l'elaborazione di metodi sempre più efficaci per rubarle o per appropriarsi di risorse per minarle. Le tecnologie emergenti, come l'intelligenza artificiale, ampliano, inoltre, la velocità, la portata e la sofisticazione del crimine organizzato, creando un panorama delle minacce ancora più complesso. In particolare, la clonazione vocale basata su IA e i *deepfake* video in tempo reale generano nuove forme di frode, estorsione e furto d'identità (R. M. V.).

Il testo del report è consultabile al seguente link

5. "The 2025 Crypto crime report": Il ruolo crescente della criptovaluta in tutte le forme di criminalità

Il report, pubblicato nel mese di febbraio 2025, evidenzia come le criptovalute siano sempre più utilizzate per finanziare e facilitare ogni tipo di attività illecita, integrante anche reati tradizionali, che in precedenza rimanevano esclusi, dato l'utilizzo illecito delle criptovalute soprattutto nell'ambito della criminalità

informatica. Si parla infatti di ransomware, mercati darknet, truffe, fondi rubati, estremismo e criminalità organizzata. Il rapporto evidenzia la necessità di una collaborazione internazionale e di strumenti avanzati di analisi blockchain per combattere il crimine legato alle criptovalute. La trasparenza delle blockchain offre opportunità uniche per tracciare e interrompere le attività illecite, ma richiede un impegno continuo da parte di governi, istituzioni finanziarie e aziende private. (Li.Pe.).

Il report è disponibile al seguente link

6. Rapporto congiunto Eurojust ed Europol "The SIRIUS-EU Eletronic Evidence legislative package"

Il report SIRIUS, pubblicato l'1 novembre 2024, mette in evidenza i progressi e le difficoltà legate all'accesso alle prove elettroniche nelle indagini penali all'interno dell'Unione Europea, dopo l'adozione nel 2023, del pacchetto legislativo dell'UE sulle prove elettroniche (*EU Electronic Evidence legislative package*), rappresentato dal Regolamento europeo 2023/1543 e dalla Direttiva europea 2023/1544. Questa nuova legislazione ha segnato un importante passo avanti, stabilendo in modo puntuale come gli Stati membri e i fornitori di servizi debbano riadattare le procedure già esistenti in tema di acquisizione, conservazione, circolazione delle prove elettroniche. Tuttavia, tali novità legislative verranno applicate gradualmente, per quanto riguarda la Direttiva dal momento della sua attuazione da parte degli Stati membri e per quanto riguarda il Regolamento solo nel 2026. Pertanto, permangono sfide legate alla rapida evoluzione delle tecnologie e alla frammentazione del quadro giuridico. L'obiettivo del progetto SIRIUS, quindi, è quello di assistere le Forze dell'Ordine e le autorità giudiziarie dell'UE nel processo di richiesta ai fornitori di servizi di dati necessari per lo svolgimento delle indagini penali, favorendo la cooperazione tra le diverse parti interessate. (Li.Pe.).

Il report è disponibile al seguente link

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. D.lgs. 27 dicembre 2024, n. 204, di adeguamento della normativa nazionale alle disposizioni del Regolamento UE/2023/1113 riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività.

Con il sopraindicato intervento è stato modificato il corredo definitorio del d.lgs. 231/2007, c.d. T.U. Antiriciclaggio, essendo stata sostituita la nozione di valuta virtuale con quella di cripto attività, individuata per rimando al regolamento UE 2023/1114, che stabilisce norme uniformi per gli emittenti di cripto-attività (c.d. *MiCA)*, tranne che si tratti delle categorie di cripto-attività di cui all'articolo 2, paragrafi 2, 3 e 4, del medesimo regolamento oppure che la cripto-attività sia altrimenti qualificata come fondi.
Conformemente a questa modifica è altresì stata riveduta la nozione di "operazione", ora inclusiva del riferimento alle cripto-attività, e sono stati individuati come obbligati, in sostituzione dei precedenti prestatori di servizi in valute virtuali, i prestatori di servizi in cripto attività, ai sensi del procedimento definito dall'art. 59 del Regolamento *MiCA*, tranne quando prestano attività di consulenza.
Per questi soggetti sono fissate apposite misure per la valutazione dei rischi associati ai trasferimenti di cripto-attività diretti a (o provenienti da) un indirizzo auto-ospitato nonché per l'esecuzione degli obblighi di adeguata verifica rafforzata della clientela nei rapporti di corrispondenza transfrontalieri che comportino l'esecuzione di servizi per le cripto-attività. Nello specifico, per "indirizzo auto-ospitato" si intende quello definito dall'art. 3, punto 20), del regolamento *MiCA* e quindi un indirizzo nel registro distribuito non collegato né ad un prestatore di servizi per le cripto né ad un soggetto che presta servizi analoghi stabilito fuori dall'Unione Europea.
Ulteriori disposizioni apposite estendono, altresì, ai prestatori di servizi per le cripto-attività gli oneri di comunicazione dei dati afferenti ai trasferimenti, da o verso l'estero, di mezzi di pagamento effettuati anche in cripto-attività, di importo pari o superiore a 5.000 euro, per conto o a favore di persone fisiche, enti non commerciali e di società semplici e associazioni equiparate (R. M. V.).

Il testo del decreto è consultabile al seguente link

2. Il disegno di legge in materia di Intelligenza Artificiale giunge all'esame della Camera dei deputati

Dopo l'approvazione, da parte del Senato in data 20.3.2025, del d.d.l. n. 1146 presentato dal Governo nell'aprile 2024, contenente "*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*", il testo - al quale sono state apportate diverse modifiche durante l'esame in Commissione in sede referente - è ora passato alla Camera dei deputati, ove ha preso il n. 2316, ed è adesso all'esame delle Commissioni.
Sui suoi contenuti, che vanno dall'enunciazione delle finalità, delle definizioni, dei principi generali (Capo I) a misure di settore (Capo II), che comprendono il sostegno alla ricerca e allo sviluppo dei sistemi di intelligenza artificiale, e vanno dal lavoro, alle professioni, dalle pubbliche amministrazioni all'attività giudiziaria (art. 15), si può consultare, per l'illustrazione articolo per articolo, il *dossier* a cura del Servizio studi del Senato del 20.3.2025, in cui si dà conto anche delle varie modifiche finora apportate.
Le norme dovrebbero naturalmente adeguare l'ordinamento interno e comunque conformarsi al recente regolamento UE 2024/1689 del 13 giugno 2024 sull'intelligenza artificiale (cd. *AI Act*, già in vigore, anche se molte sue disposizioni saranno applicabili solo in tempi successivi). Tuttavia, l'art. 3, comma 5, si limita a stabilire che "*la presente legge non produce nuovi obblighi rispetto a quelli previsti dal regolamento* europeo.
Dal punto di vista del diritto penale, rileva innanzitutto il Capo V, composto dal solo art. 26, che prevede modifiche al codice penale, concernenti l'introduzione di una nuova aggravante comune (art. 61, n. 11-*decies*) se il fatto è commesso "*mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato*". Inoltre, si prevede l'introduzione di un nuovo delitto, all'art. 612-*quater* c.p., inserito fra quelli contro la persona, diretto a punire, sotto la rubrica "*illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale*" il fenomeno del c.d. *deep fake*.
Altre circostanze aggravanti speciali sono poi previste per singoli delitti, anche extra codice.
Ma rileva anche l'art. 24, che contiene molteplici deleghe legislative, fra cui, al comma 5, lett. b) e c), quelle con cui si stabilisce che si introducano "*autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sull'omessa adozione o sull'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, quando da tali omissioni deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato*", nonché che vengano "*precisati*" dei "*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*". Peraltro non vi è alcuna indicazione su quali possano essere questi criteri di imputazione.
Indirettamente possono, infine, influire sull'applicazione di diverse fattispecie penali altre disposizioni, relative a diversi settori, fra cui quelle in materia di diritto d'autore (art. 15), in materia di cybersicurezza (art. 18) ed in materia sanitaria (artt. 7-11), che vanno in particolare dalla "*ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario*" (art. 8) al "*trattamento dati personali per finalità di ricerca e sperimentazione*" (art. 9), nonché gestione del fascicolo sanitario elettronico (art. 10). Queste disposizioni possono fra l'altro delimitare le fattispecie penali che incriminano il trattamento illecito di dati personali (art. 167 Codice privacy) e la loro comunicazione e diffusione illecite su larga scala (art. 167-*bis* Codice privacy), rispetto ai quali è da segnalare anche la disciplina del più recente regolamento (UE) 2025/327 dell'11.2.2025 sullo "*spazio europeo dei dati sanitari*" (*EHDS Act*).

Il testo del Regolamento (UE) 2025/327 è consultabile al seguente link.
Il testo del d.d.l. "*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*" è disponibile al seguente link.

Per alcuni aggiornati riferimenti sui riflessi penali in ambito sanitario, si veda nella bibliografia sottostante. (L.P.)

3. D.lgs. 10 marzo 2025 n. 23 di adeguamento della normativa nazionale alle disposizioni del regolamento UE/2022/2554, c.d. DORA.

Conformemente al regolamento sopra indicato, sulla resilienza operativa digitale del settore finanziario, il decreto in esame individua, come autorità di sorveglianza sugli obblighi imposti, la Banca d'Italia, la Consob,

l'IVASS e il COVIP, che sono designate, insieme al CSIRT Italia, ovvero l'organo dell'Agenzia per la Cybersicurezza Nazionale, anche come destinatari per le segnalazioni di gravi incidenti informatici occorsi e per le segnalazioni di minacce informatiche significative. Le autorità di vigilanza sono, inoltre, destinatarie di appositi poteri regolamentari ed ispettivi, potendo anche imporre alle entità finanziarie di sospendere temporaneamente, in tutto o in parte, l'utilizzo o l'introduzione di un servizio prestato dal fornitore terzo critico di servizi TIC o eventualmente di risolvere gli accordi contrattuali. Relativamente al fornitore, l'autorità può effettuare accessi e ispezioni e richiedere documenti. Sul piano sanzionatorio, l'art. 10, intervenendo direttamente sugli artt. 144 e 144 ter del Testo Unico Bancario, prevede sanzioni amministrative pecuniarie differenziate per soggetto e per tipologia di violazione. Costituiscono, in particolare, violazioni gravi quelle relative alle governance e all'organizzazione, al quadro per la gestione dei rischi informatici o al processo di gestione degli incidenti connessi alle TIC nonché di segnalazione dei gravi incidenti. Per le violazioni gravi le sanzioni vanno per istituti di pagamento da euro 30.000 fino a euro 3,5- 5 milioni ovvero, nei confronti dei soggetti sottoposti al TUF, fino a 20 milioni oppure fino al 7% o il 10% del fatturato. Variano conformemente anche le sanzioni applicabili ai fornitori di servizi TIC, che sono parametrate, in ogni caso, in base al soggetto al quale vengono erogati i propri servizi. E' inoltre previsto che quando l'inosservanza sia conseguenza della violazione dei doveri propri del soggetto apicale o dell'organo di appartenenza e la condotta abbia inciso sull'organizzazione o sui profili di rischio aziendali o abbia contribuito a determinare la violazione da parte dell'ente, siano anche sanzionati i predetti apicali con pene pecuniarie da 5.000 Euro fino a 5 milioni, in caso di condotte più gravi, e con la misura accessoria dell'interdizione, per un periodo non inferiore a sei mesi e non superiore a tre anni, dallo svolgimento di funzioni di amministrazione, direzione e controllo presso intermediari e imprese autorizzati ai sensi del TUF, del TUB, del Codice delle Assicurazioni Private (R.M. V.).

Il testo del decreto è consultabile al seguente link

4. Proposta di legge: "*Modifica alla legge 4 aprile 1956, n. 212, e altre disposizioni per prevenire l'alterazione o la manipolazione delle campagne elettorali e referendarie attraverso la diffusione di contenuti ingannevoli prodotti mediante sistemi di intelligenza artificiale*"

In data 23 gennaio 2025, con Atto della Camera dei deputati, n. 2212, è stata presentata la proposta di legge volta alla modifica della legge n. 212/1956, che disciplina il periodo del c.d. "silenzio elettorale". Il divieto di propaganda elettorale, ad oggi, non può essere applicato ai social network e ad altri strumenti telematici che non sono espressamente menzionati in suddetta legge. Si è pertanto avvertita l'esigenza, soprattutto negli ultimi anni, data la diffusione di una particolare categoria di intelligenza artificiale generativa, che produce *deepfake,* di introdurre un'apposita disciplina che punisca la diffusione di contenuti ingannevoli, in grado di manipolare la veridicità dell'informazione durante il periodo elettorale e, dunque, di alterare le sorti della votazione. L'Atto della Camera propone di introdurre all'interno della legge n. 212/1956, l'art. 9-novies, volto a sanzionare penalmente "*chiunque al fine di alterare il libero svolgimento delle campagne elettorali o referendarie o di manipolarne il risultato, cede, pubblica o altrimenti diffonde contenuti ingannevoli o manipolati generati in tutto o in parte con sistemi di IA*", punendolo con la reclusione da uno a quattro anni (Li.Pe.).

Il testo della proposta di legge è consultabile al seguente link

5. *Rapporto Clusit sulla Cybersecurity in Italia e nel mondo 2025*

Il rapporto sulla cybersecurity in Italia e nel mondo, pubblicato nel marzo 2025, analizza l'evoluzione del cyber crime, le normative e le misure di protezioni assunte, focalizzandosi sull'aumento degli attacchi, divenuti ora più gravi e preoccupanti, per cui è sempre più importante agire in prevenzione adottando una politica di sicurezza anche cibernetica a tutti i livelli.
A livello globale, la crescita degli attacchi *noti* rispetto al 2023 è stata del 27%, evidenziando una situazione critica a livello internazionale, dovuta anche al conflitto in Ucraina, che ha innestato una nuova fase definita di "guerra cibernetica diffusa" dal 2022. Il Cybercrime si conferma la principale causa degli incidenti, con oltre l'86%, seguito da attività di hacktivism generalizzata (8%), di espionage/sabotage (4%) ed information Warface (2%), mentre le principali vittime sono multipli bersagli (per il 17,8%), enti governativi e la sanità (che condividono la percentuale del 13,3%), relegando sotto al 10 % le attività finanziarie, l'educazione, il manufacturing, le news ed i media, ecc.

In Italia, invece, la percentuale di crescita degli attacchi è del 15,2% rispetto all'anno precedente, attestandosi polarmente tra incidenti di Cybercrime (per il 78%) e di hacktivism (per il 22%), verso bersagli in prevalenza di news/multimedia (per il 18%), mentre manufacturing è al secondo posto (con il 16%) degli attacchi, seguito da Government (10% del totale), che nel 2023 occupava il vertice della graduatoria.
Il report ha, inoltre, registrato oltre 69 milioni di eventi di sicurezza, caratterizzato da un aumento vertiginoso di infezioni da malware (+ 131%), di attacchi DDoS (del 100%) con un incremento del 167% della distribuzione della banda aggregata media in Tbps e una crescita marcata degli attacchi di maggiore intensità (>100 Gbps), nonchè di attacchi alla Pubblica amministrazione (+ 155%).
Le sfide future includono la crescente pressione degli attacchi e l'adeguamento alle normative in evoluzione, per cui è cruciale implementare pratiche di *security by design* e migliorare i processi di gestione degli incidenti. La cultura della sicurezza deve essere sviluppata in sinergia tra scuole, università e soggetti pubblici e privati, per garantire un ecosistema sicuro per tutti. (S.T.)

Il testo del rapporto è consultabile al seguente link

NOVITÀ GIURISPRUDENZIALI NAZIONALI ED EUROPEE

1. *Atti persecutori da intrusione informatica-telematica*

Per la Corte di Cassazione il "perdurante e grave stato di ansia e di paura" che rappresenta l'evento del reato di atti persecutori può essere certamente causato da una costante sorveglianza ed ingerenza nella sfera più intima della persona offesa attraverso il ricorso a tecnologie informatiche e telematiche. Nel caso esaminato, è pertanto stata confermata la qualificazione come persecutorie delle condotte di clonazione ed accesso abusivo al profilo *Facebook* della vittima e l'utilizzo dei *frames*, tratti dall'impianto di videosorveglianza collocato in prossimità dell'ex abitazione familiare, per l'indebito ed assillante controllo della vita e della riservatezza della ex compagna. Non si tratta, per la Corte, di semplice "molestie", ma di comportamenti oppressivi e di prorompente efficacia intromissiva idonei a generare gli eventi completati dall'art. 612 *bis* c.p. (R. M. V.)

Cassazione penale, Sez. V, 14 marzo 2025, n. 10362

2. *La Cassazione si pronuncia ancora sulla c.d. violenza sessuale telematica*

La Suprema Corte ha ribadito che il reato di violenza sessuale può configurarsi indipendentemente da un contatto fisico tra l'agente e la vittima allorquando venga lesa la capacità di autodeterminazione di quest'ultima per essere stata costretta, mediante violenza o minaccia (art. 609 bis primo comma), ovvero indotta (art. 609 bis secondo comma) alla profanazione della sua sfera sessuale. Pertanto, configura il reato di violenza sessuale anche il costringere la vittima a compiere e filmare atti di autoerotismo dietro la minaccia di diffondere il video di un precedente rapporto sessuale della vittima. (C.C.)

Conformi: Sez. 3, Sentenza n. 26809 del 04/04/2023; Sez. 3, Sentenza n. 11958 del 22/12/2010 - dep. 24/03/2011, Rv. 249746; Sez. 3, Sentenza n. 25822 del 09/05/2013, Rv. 257139; Sez. 3, n. 41951 del 05/07/2019.

Cassazione penale, Sez. III – 12 febbraio 2025, n. 5688

3. *L'accesso abusivo a sistema informatico o telematico*

La Corte ha ritenuto configurabile il reato di cui all'art. 615-*ter* c.p. anche nel caso in cui l'ex coniuge, in possesso del PIN del proprietario dello *smartphone*, vi acceda al fine di prendere cognizione della corrispondenza ivi contenuta, qualora la condotta incriminata abbia portato ad un risultato certamente in contrasto con la volontà della persona offesa ed esorbitante l'eventuale ambito autorizzatorio. Inoltre, ha escluso che per tale condotta possa essere riconosciuta la causa di giustificazione di avere agito in adempimento del dovere di genitore di tutelare la salute del minore in periodo pandemico. (C.C.)

Cassazione penale, Sez. V, 27 gennaio 2025, n. 3025

4. *L'invio ripetuto di messaggi Whatsapp integra il reato di molestia*

In tema di reato di molestia o disturbo alle persone ai sensi dell'art. 660 cod. pen., l'invio ripetuto di messaggi telefonici tramite SMS o WhatsApp può configurare un'effettiva e significativa intrusione nell'altrui sfera personale, e come tale è sanzionabile, a prescindere dal contenuto dei messaggi stessi. Differente è il caso delle comunicazioni tramite posta elettronica, le quali non configurano il reato in oggetto, in quanto non costituiscono intrusione forzata nella libertà del destinatario, che può scegliere liberamente di leggere o meno tali messaggi. (Li.Pe.).

Cassazione penale, Sez. I, 21 gennaio 2025, n. 8231

5. *Limiti all'acquisizione nel processo penale della messaggistica istantanea mediante screenshot*

Per la Suprema Corte, ai fini dell'acquisizione, da parte della Polizia giudiziaria di messaggistica istantanea archiviata nei dispositivi elettronici, non è sufficiente il consenso dell'avente diritto, neppure se informato della facoltà di farsi assistere da un difensore, ma è necessario un provvedimento dell'autorità giudiziaria, ai sensi dell'art. 254 c.p.p.. La Polizia giudiziaria non può avere accesso diretto al contenuto delle *chat*, ma solo acquisire materialmente il dispositivo elettronico in cui sono contenute. (Li.Pe.)

Cassazione penale, Sez. VI, 13 gennaio 2025, n. 1269

6. *Insulti in diretta sui social network: la telefonata non è diffamatoria*

La telefonata dal contenuto offensivo, diffusa sul proprio profilo "aperto" di Facebook dall'imputato mentre era in contatto con la persona offesa, integra il delitto di ingiuria aggravata dalla presenza di più persone, depenalizzato ai sensi dell'art. 1, comma 1, lett. c) D.Lgs. 15 gennaio, n. 7, e non il delitto di diffamazione. Ciò in quanto l'imputato aveva pronunciato espressioni offensive mediante comunicazioni telematiche dirette alla persona offesa attraverso un video chat, fruibile da terzi, quindi con contestualità tra la pronuncia degli appellativi e le frasi offensive ed il recepimento delle stesse da parte del destinatario. Pertanto, il discrimine tra i due delitti è la circostanza che nell'ingiuria la comunicazione, con qualsiasi mezzo realizzata, è diretta all'offeso, mentre nella diffamazione l'offeso resta estraneo alla comunicazione intercorsa con più persone e non è posto in condizione di interloquire con l'offensore.
Non è, in ogni caso, argomento a sostegno della sussistenza della diffamazione la circostanza che la pubblicazione del video sia rimasta a lungo sulla bacheca dell'imputato, essendo questo un delitto di evento, che si consuma nel momento e nel luogo in cui i terzi percepiscono l'espressione offensiva; mentre nel caso in cui frasi o immagini lesive siano state immesse in un canale telematico, la consumazione avviene nel momento in cui il collegamento viene attivato, perché è in quel momento che esse diventano fruibili da parte dei terzi, essendo inserite in un ambiente comunicativo per sua natura destinato a essere normalmente visionato da più persone. (S.T.)

Cass. pen., Sez. V, Sent., (data ud. 13/12/2024) 28/02/2025, n. 8341

7. *Diffamazione a mezzo stampa telematica: locus commissi delicti*

La giurisprudenza di legittimità formatasi in materia di *locus commissi delicti* del delitto di diffamazione, qualificandolo quale di reato di evento, ha riconosciuto che la sua consumazione si ha nel momento e nel luogo in cui i terzi - almeno due - percepiscono l'espressione ingiuriosa; ciò in particolare quando un secondo soggetto ne apprenda il contenuto lesivo dell'onore e della reputazione della persona offesa.
In tema di diffamazione a mezzo stampa telematica, la Cassazione ribadisce che non trova applicazione il tradizionale criterio interpretativo in tema di stampa cartacea, che valorizza il luogo di prima divulgazione del giornale – che corrisponde al luogo di stampa o in cui è situata la tipografia – quale *locus commissi delicti*, con evidenti riflessi sulla competenza territoriale.

In linea esegetica, trattandosi di reato di evento, la condotta di immissione del contenuto diffamatorio in uno spazio informatico o telematico (nel caso analizzato, uno spazio web) non consolida l'evento di offesa alla reputazione, essendone ontologicamente da questo distinta, poiché l'evento si concretizza solo quando almeno due visitatori prendano visione del contenuto. Pertanto, il *locus* così individuato sarebbe quello in cui i terzi effettivamente apprendono la notizia lesiva. Tuttavia si tratta, in tutta evidenza nel mondo virtuale di ampiezza planetaria, di un accertamento estremamente complicato se non impossibile.
Trovandosi nell'impossibilità tecnica di superare quest'impasse, la Corte ha dunque riaffermato – ribadendo l'orientamento giurisprudenziale formatosi grazie alla storica pronuncia delle Sezioni Unite c.d. Rocco in tema di accesso abusivo a sistema informatico o telematico – che per individuare il *locus commissi delicti*, al fine di stabilire la competenza per territorio, debba aversi riguardo al luogo in cui è avvenuto il caricamento del dato informatico che contiene l'espressione diffamatoria, trattandosi questo dell'ultimo luogo conoscibile in cui è avvenuta una parte dell'azione che incorpora uno degli elementi costitutivi della fattispecie. In via gradata, ove tale accertamento non fosse praticabile, si dovrà ricorrere ai criteri suppletivi di cui all'art. 9, comma secondo, c.p.p., quali il luogo di residenza, domicilio o dimora dell'imputato. (S.T.)

Cass. pen., Sez. V, Sent., (data ud. 07/03/2025) 10/04/2025, n. 14204

8. Sequestro di dati informatici: è sufficiente il decreto del Pubblico Ministero

In tema di sequestro probatorio, sia pure con riferimento ad indagini relative al delitto di diffusione illecita di immagini o video sessualmente espliciti di cui all'art. 612-*ter* cod. pen. commesso mediante accesso alla "rete", la Cassazione ribadisce che l'attività della Polizia giudiziaria non necessita di convalida nel caso in cui il decreto del Pubblico Ministero disponga, senza ulteriori specificazioni, l'ablazione di dispositivi informatici in uso all'indagato, in quanto, trattandosi di beni correlati alla tipologia del reato per cui si procede, l'indicazione degli stessi non lascia spazio alla discrezionalità degli operanti. È sufficiente, infatti, che la motivazione consenta agli operanti di comprendere l'oggetto del sequestro e l'aspettativa del rinvenimento di ciò che si ricerca ai fini di prova attraverso le cose sequestrate, in specie i dati informatici contenuti all'interno dei dispositivi: dati che, anche in base al dettato della pronuncia n.170/2023 della Corte costituzionale, erano rappresentati da scambi di messaggi elettronici (come e-mail, SMS, WhatsApp e simili). Questi, trattandosi di messaggi già ricevuti e letti dal destinatario, quindi conservati nella memoria di un dispositivo elettronico, si trasformano in mero documento "storico", pertanto acquisibili nelle forme previste dall'art. 254 c.p.p. (S.T.)

Cass. pen., Sez. V, Sent., (data ud. 28/01/2025) 28/02/2025, n. 8376

9. Allucinazioni di I.A. nella giurisprudenza civile: l'ordinanza del Tribunale di Firenze

Il Tribunale adito, in un procedimento cautelare di tutela del diritto di proprietà industriale, ha ritenuto di rigettare la richiesta di condanna per lite temeraria, *ex* art. 96 c.p.c., avanzata da una parte per avere l'altra indicato, in sede di comparsa di costituzione, sentenze inesistenti ovvero di contenuto reale non corrispondente a quello riportato.
Lo strumento *"ChatGPT"*, utilizzato all'oscuro dalla collaboratrice del difensore di una delle parti costituite, ha inventato precedenti di asserite pronunce della Corte di Cassazione afferenti al caso controverso, ma che, in verità, rappresentavano precedenti del tutto fantasiosi, tanto da ricondurre quanto verificatosi al fenomeno delle cc.dd. allucinazioni di intelligenza artificiale. Questo si verifica allorché l'I.A. inventi risultati inesistenti ma che, anche a seguito di una seconda interrogazione, vengono confermati come veritieri.
Il Collegio procedente, pur riconoscendo il disvalore dell'omessa verifica dell'effettiva esistenza delle sentenze risultanti dall'interrogazione dell'I.A., le ha ritenute quale mero strumento rafforzativo della strategia difensiva della parte, già nota anche nei giudizi di merito; mentre ha escluso che il loro utilizzo fosse finalizzato a resistere in giudizio con malafede, con colpa grave o con una condotta processuale di abuso della funzionalità del servizio di giustizia. (S.T.)

Trib. Ordinario di Firenze, Sez. Imprese, Ord. 14 marzo 2025

NOVITÀ RILEVANTI A LIVELLO NAZIONALE

1. Relazione annuale Intelligence 2025 al Parlamento sulla Politica dell'Informazione per la Sicurezza

Il documento redatto dall'organizzazione "Sistema di informazione per la sicurezza della Repubblica" affronta la crescente complessità delle minacce cyber alla sicurezza nazionale. Un aspetto importante trattato dalla Relazione riguarda l'innovazione tecnologica, che, da un lato, offre nuove opportunità di sviluppo, ma dall'altro apre anche nuovi spazi di vulnerabilità. In particolare, la trasformazione digitale e la crescente interconnessione dei sistemi sociali e tecnologici hanno amplificato le possibilità di attacchi da parte di attori ostili. Si registra, infatti, un aumento degli attacchi alle amministrazioni centrali dello Stato, con particolare riguardo alle infrastrutture digitali, dell'energia e dei trasporti. Un altro elemento significativo della Relazione riguarda l'attenzione crescente verso l'intelligenza artificiale (IA). L'IA rappresenta sia un'opportunità, grazie alla sua capacità di velocizzare e migliorare l'attività di Intelligence, che una potenziale minaccia per la sicurezza delle democrazie, in particolare per il suo impatto sul lavoro, sulle applicazioni militari e sulla gestione dell'informazione. La Relazione evidenzia anche i rischi legati all'eccesso di informazioni disponibili online, che rende necessario un continuo adattamento dei processi e degli strumenti di Intelligence. (Li.Pe.).

La relazione è disponibile al seguente link

2. Comunicato stampa della decisione del Garante Privacy nei confronti di OpenAI

Il 20 dicembre 2024, il Garante per la protezione dei dati personali ha pubblicato un comunicato stampa riguardante l'adozione di un provvedimento correttivo e sanzionatorio nei confronti di OpenAI, datato 2 novembre 2024, in relazione alla gestione del servizio ChatGPT. Secondo il Garante la società statunitense, che ha creato e gestisce il chatbot di intelligenza artificiale generativa, oltre a non aver notificato all'Autorità la violazione dei dati subita nel marzo 2023, ha trattato i dati personali degli utenti per addestrare ChatGPT senza aver prima individuato un'adeguata base giuridica e ha violato il principio di trasparenza e i relativi obblighi informativi nei confronti degli utenti. Per di più, OpenAI non ha previsto meccanismi per la verifica dell'età, con il conseguente rischio di esporre i minori di 13 anni a risposte inidonee rispetto al loro grado di sviluppo e autoconsapevolezza. L'Autorità, con l'obiettivo di garantire, innanzitutto, un'effettiva trasparenza del trattamento dei dati personali, ha ordinato a OpenAI, utilizzando per la prima volta i nuovi poteri previsti dall'articolo 166, comma 7 del Codice Privacy, di realizzare una campagna di comunicazione istituzionale di 6 mesi su radio, televisione, giornali e Internet. Inoltre, il Garante ha comminato a OpenAI una sanzione di quindici milioni di euro. (Li.Pe.).

Il comunicato stampa è disponibile al seguente link

VOLUMI E CONTRIBUTI DOTTRINALI DI RILIEVO

Diritto penale e processo

Balsamo A., *Spazio virtuale e processo penale: la nuova Convenzione ONU sul cybercrime*, n. 2/2025, p. 240 ss.

Mattarella A., *Diritto penale e nuove tecnologie: dalla Convenzione ONU contro i reati informatici alle sfide dell'Intelligenza Artificiale*, n. 2/2025, p. 250 ss.

Giurisprudenza penale

Macri L., *I primi passi dell'Italia verso l'impiego dell'IA nel processo penale e il calcolo del rischio di recidiva*, n. 2, 2025.

La legislazione penale

Della Torre J., *Spunti in tema di cripto-attività e procedimento penale*, 28 febbraio 2025, p. 1 ss.;

Della Torre J. Ponteprino G., *Commento al d.lgs. 129 del 2024 di attuazione del regolamento UE sui mercati delle cripto-attività. Le novità sul versante penalistico e amministrativo punitivo*, 18 febbraio 2025, p. 1 ss.

Processo penale e giustizia

Santoro E.L. *L'ispezione informatica sul telefono cellulare già colpito da un sequestro annullato: un caso di carenza del potere di acquisizione della prova*, fascicolo 2-2025.

Responsabilità sanitaria

Picotti L.*, Impiego di sistemi d'intelligenza artificiale in medicina e digitalizzazione dei dati sanitari: possibili profili di rilevanza penale*, in *Responsabilità sanitaria*, 30 aprile 2025 p. 122-134.

Sistema Penale

Lombardi O., *Responsabilità penale dell'uomo per il danno cagionato attraverso condotte dolose e colpose nell'impiego dei sistemi di intelligenza artificiale*, 4 dicembre 2024.

Parodi L., *La "gravità dell'ingerenza" nel prisma della proporzionalità: nuovi equilibri in tema di data retention*, 7 marzo 2025.

Articoli in altre riviste

Crescioli C., *La lucha contra el cibercrimen y las últimas reformas penales en España e Italia: luces y sombras*, in *Revista de Estudios Jurídicos y Criminológicos*, 2024, n. 10, p. 403 ss.

Crescioli C., *La delincuencia organizada en el Sistema Penal Italiano y las nuevas tecnologías*, in *Revista Argentina de Derecho Penal y Procesal Penal*, 2024, n. 36, p. 1 ss.

Contributi in volumi

Picotti L., *Artificial Intelligence and Criminal Law*, in Anzenberger P., Schwaighofer K. (Hrsg), *Recht der Digitalisierung II*, Mohr Siebeck Tuebingen, 2025, p. 1 ss.

Volumi

Vadalà R. M., *La fattispecie penale tra economia digitale e diritto europeo*, Giappichelli, gennaio 2025.

Iaselli M., *Le nuove regole per l'uso primario e secondario dei dati sanitari - Reg. UE 11 febbraio 2025, n. 327 (EHDS)*, Maggioli Editore, 2025.