CYBER- and A.I.- CRIME

Rassegna delle novità (aprile 2024 – novembre 2024)

Rassegna di novità in materia di diritto e processo penale e nuove tecnologie

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

NOVITÀ SOVRANAZIONALI

1. *AI Act*: entrato in vigore il Regolamento europeo 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale

In data 1° agosto 2024 è entrato in vigore il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, 2016/797/UE e 2020/1828/UE (regolamento sull'intelligenza artificiale, od AI Act, pubblicato in GUUE del 12.07.2024, serie L. It.
Per alcuni primi riferimenti sul rilievo che può avere anche dal punto di vista della responsabilità penale si veda L. Picotti, *Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palingenesi? Le raccomandazioni dell'*Association Internationale de Droit Pénal *e la rilevanza del recente regolamento europeo sull'intelligenza artificiale*, in *Sistema penale*, 31.7.2024. *(L.P.)*

Il testo dell'AI Act è disponibile in versione italiana al seguente link

2. Direttiva 2024/1385 del 14 maggio 2024 sulla lotta alla violenza contro le donne e alla violenza domestica

La Direttiva 2024/1385 si pone in continuità con il quadro delineato dalla Convenzione di Istanbul dell'11 maggio 2011 adottata dal Consiglio d'Europa, riguardante la prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica e con i successivi interventi dell'Unione europea nello sforzo di fornire una migliore risposta, sul piano preventivo e repressivo, ad un fenomeno (quello della violenza di genere) in preoccupante espansione.
Tale Direttiva stabilisce delle norme minime riguardanti la definizione dei reati e delle sanzioni in materia di sfruttamento sessuale femminile e minorile e di criminalità informatica; i diritti delle vittime di tutte le forme di violenza contro le donne o di violenza domestica prima, durante e per un congruo periodo dopo il procedimento penale; la protezione e l'assistenza delle vittime, la prevenzione e un intervento precoce.
Nel Capo II vengono indicate le condotte che gli Stati membri devono necessariamente punire come reati: la mutilazione dei genitali femminili; il matrimonio forzato; la condivisione di materiale intimo o manipolato (c.d. *deepnude*); la condotta di stalking perpetrata online; l'istigazione alla violenza e all'odio online.
In particolare, si ritiene di richiamare all'attenzione l'interesse espresso dal legislatore europeo nel penalizzare le condotte perpetrate attraverso l'uso delle tecnologie dell'informazione e della comunicazione («TIC»), che trovano massima espressione nell'art. 5, lettera b) della Direttiva 2024/1385, che stabilisce il dovere per gli Stati membri di adottare un'apposita fattispecie di reato per i c.d. *deepnude* ovvero immagini o video in cui la persona raffigurata viene "spogliata" artificialmente attraverso appositi sistemi di Intelligenza Artificiale. Viene in tal modo enfatizzato l'effetto aggravante della dannosità del reato perpetrato attraverso mezzi informatici. *(Li. Pe.)*

Il testo della direttiva è disponibile al seguente link

3. *AML Package*: le nuove prescrizioni antiriciclaggio

Il 19 giugno 2024 è stato pubblicato in Gazzetta Ufficiale dell'Unione Europea il c.d. "AML Package", che comprende la VI Direttiva Antiriciclaggio, il Regolamento Antiriciclaggio o c.d *single Rulebook* e il Regolamento di istituzione della nuova Autorità Antiriciclaggio.
In particolare, con il Regolamento Antiriciclaggio è stata estesa la platea dei soggetti obbligati del settore delle cripto-attività ed incluse le piattaforme di crowdfunding, i soggetti che commerciano beni di lusso e le società e gli agenti nel settore del calcio professionistico. Anche questi soggetti saranno tenuti ad osservare le norme immediatamente applicabili in tema di *due diligence* sulla clientela e trasparenza dei titolari effettivi. *(R.M.V.)*

L'*AML Package* nei vari atti che lo compongono è consultabile al seguente link

4. Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale

Il Consiglio d'Europa ha adottato, in data 5 settembre 2024 una nuova convenzione su "Artificial Intelligence and Human Rights, Democracy and the Rule of Law". Si tratta del primo trattato internazionale giuridicamente vincolante sull'IA ed è pienamente in linea con il regolamento europeo 2024/1689 sull'IA.
La convenzione prevede un approccio comune per garantire che i sistemi di IA siano compatibili con i diritti umani, la democrazia e lo Stato di diritto, consentendo nel contempo l'innovazione e la fiducia. Comprende una serie di concetti chiave tratti dal regolamento dell'UE sull'IA, tra cui un approccio basato sul rischio, trasparenza lungo la catena del valore dei sistemi di IA e dei contenuti generati dall'IA, obblighi di documentazione dettagliata per i sistemi di IA identificati come ad alto rischio e obblighi di gestione dei rischi con possibilità di introdurre divieti per i sistemi di IA considerati una chiara minaccia per i diritti fondamentali. Dovrà firmata e ratificata da almeno cinque Stati parte per entrare formalmente in vigore. *(L.P.)*

Il testo della Convenzione è disponibile al seguente link

5. *Cyber resilience Act*. Approvato il Regolamento europeo 2847 del 23 ottobre 2024

Il 23 ottobre 2024 è stato approvato il Regolamento europeo relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza).
L'obiettivo del Regolamento è rafforzare le norme sulla sicurezza informatica per garantire prodotti hardware e software più sicuri, cercando di fornire una risposta a due importanti problemi: un basso livello di sicurezza informatica e una scarsa comprensione delle informazioni da parte degli utenti, che impediscono loro di scegliere prodotti con proprietà di cibersicurezza adeguate o di utilizzarli in modo sicuro. Per questo motivo, sono stati definiti quattro obiettivi specifici: garantire che i produttori migliorino la sicurezza dei prodotti con elementi digitali fin dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita; garantire un quadro coerente di sicurezza informatica, facilitando la conformità per i produttori di hardware e software; migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali e consentire alle aziende e ai consumatori di utilizzare in modo sicuro prodotti con elementi digitali. *(B.P.)*

Il testo del *Cyber Resilience Act (CRA)* è disponibile al seguente link

6. Report Europol *AI and policing*: benefici e sfide dell'intelligenza artificiale nell'attività investigativa del 23 settembre 2024

Il report indaga approfonditamente le applicazioni dell'IA nel campo dell'attività investigativa e d'indagine, esaminando alla luce del contesto regolamentare inaugurato dell'*Artificial Intelligence Act (supra sub 1)* le criticità relative a *data bias* e discriminazioni e le minacce alla *privacy* ed alla protezione dei diritti umani. *(R.M.V.)*

Il report dell'Europol è reperibile al seguente link

7. Report Euipo relativo all'impatto del metaverso sulla violazione e l'applicazione della proprietà intellettuale

Il report dell'*European Union Intellectual Property Office* evidenzia come il Metaverso e le tecnologie correlate possano essere utilizzate in modo improprio, in violazione delle norme poste a tutela della proprietà intellettuale, suggerendo, quindi, di individuare nuove strategie ed adeguare la disciplina vigente alle continue sfide poste dal Metaverso. *(R.M.V.)*

Il report è reperibile al seguente link

8. Ciberspazio: il Consiglio dell'Unione europea approva una dichiarazione relativa a un'intesa comune sull'applicazione del diritto internazionale al ciberspazio

Nella dichiarazione del Consiglio dell'Unione europea del 18 novembre 2024 si afferma che il ciberspazio non è un settore privo di regolamentazione, ribadendo il rispetto e l'osservanza del quadro delle Nazioni Unite per il comportamento responsabile degli Stati che afferma l'applicabilità del diritto internazionale, ed in particolare la Carta delle Nazioni Unite, al ciberspazio. *(R.M.V.)*

La dichiarazione è reperibile al seguente link

9. Report UNICRI di giugno 2024: un uso terroristico ed estremista del dark web

Un tema centrale del rapporto è l'ascesa del "cybercrime-as-a-service" vale a dire l'offerta in Internet e nel Dark web di malware e software nonché altri dispositivi per commettere reati online (cfr. infra sub n. 11), che ha un ruolo importante nel rivoluzionare il panorama del cybercrime. Si tratta di un modello che facilita la conduzione di attacchi informatici, anche complessi, consentendo la collaborazione tra individui singoli e gruppi organizzati, con il conseguente sviluppo anche del fenomeno del terrorismo nel Cyberspace. *(R.M.V.)*

Il report UNICRI è reperibile al seguente link

10. Report UNICRI sull'AI generativa: una nuova minaccia per lo sfruttamento e l'abuso sessuale dei minori online

L'Intelligenza Artificiale generativa viene sempre più spesso impiegata nella realizzazione di contenuti pedopornografici, rendendo particolarmente difficoltosa la lotta a questo crimine. Tra le forme di AI generativa sono ricompresi anche i *deepfake,* ovvero immagini e video realizzati con sistemi informatici tali da far apparire come verosimili situazioni che non si sono mai verificate, in grado di rappresentare anche e soprattutto minori privi dei loro indumenti o che sembrano coinvolti in atteggiamenti sessualmente espliciti. L'utilizzo dell'AI generativa, ed in particolare del *deepfake*, incrementa la circolazione di materiale pedopornagrafico nel Cyberspace, anche non raffigurante minori realmente esistenti, ma comunque lesivo di un bene giuridico individuabile nel corretto sviluppo psichico, fisico, morale ed affettivo dei minori e nel rispetto della loro dignità umana. *(Li. Pe.)*

Il report UNICRI è reperibile al seguente link

11. La geografia del cybercrime: svelato l'indice mondiale della criminalità informatica

La lotta alla criminalità informatica rappresenta da decenni il primo obiettivo di governo di innumerevoli Stati nel mondo, ben consapevoli dell'impatto dannoso di milioni, se non di miliardi di euro, che genera. Nonostante lo sforzo assunto dai vari Paesi, il fenomeno del cybercrime molto spesso si sviluppa nell'ombra: i criminali informatici operano celati dai software di occultamento degli *IP address*, utilizzando *nicknames* fuorvianti od altri stratagemmi tecnici loro disponibili.
Con l'articolo in parola, recentemente pubblicato sulla rivista "*Plos One*", tuttavia, un sondaggio condotto su decine di esperti di criminalità informatica e di intelligence interrogati sul tema, ha perseguito di attribuire una localizzazione definita ai crimini informatici. Gli esperti interrogati, scelti tra i migliori "*professionisti adulti che sono stati impegnati nell'intelligence, nell'indagine e/o nell'attribuzione di crimini informatici per un*

minimo di cinque anni" aventi una reputazione eccellente, durante i *focus group* e l'indagine pilota hanno convenuto essere cinque le categorie di minacce, finanziariamente motivate, più significative realizzate dalla criminalità informatica su scala globale. Tali categorie possono essere sintetizzate in: i) prodotti/servizi tecnici (ad es. software di programmazione di malware, accesso alle botnet, accesso a sistemi compromessi, produzione di strumenti); ii) attacchi informatici ed estorsioni (es. attacchi DDoS, ransomware); iii) furto di dati/identità (ad es. *hacking, phishing*, compromissione dell'account, carte di credito incluse); iv) truffe (ad es. *advance fee fraud*, compromissione di e-mail aziendali, frode d'asta online); v) riscossione/riciclaggio di denaro (ad es. frodi con carta di credito, frodi c.d. *money mule*, piattaforme illegali di valute virtuali).
Tale studio ha portato a scoprire che un numero molto ristretto di Stati nel mondo detiene la maggior concentrazione di criminalità informatica nei sopradetti ambiti: rispettivamente Russia, Ucraina, Cina, Stati Uniti, Nigeria e Romania. A zone territoriali diverse corrispondevano categorie di reati informatici differenti. Ad esempio, i crimini informatici legati a prodotti o servizi tecnici, attacchi informatici ed estorsioni, riscossione, riciclaggio di denaro, nonché furto di dati e di identità sono stati la categoria principale in Russia; mentre le frodi informatiche in Nigeria.
Sebbene la criminalità informatica rappresenti un fenomeno certamente vasto ed esteso, avere contezza dei principali paesi in cui il crimine informatico si sviluppa rappresenta un punto di partenza importante per elaborare strategie funzionali ed efficaci per rispondere in modo adeguato all'evoluzione di questi crimini. *(S.T.)*

Lo studio è reperibile alla seguente pagina della rivista *Plos One*

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. **Legge n. 70 del 17 maggio 2024. Disposizioni e delega al governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo**

Pubblicata sulla Gazzetta Ufficiale il 30 maggio 2024, la legge n. 70 del 17 maggio 2024, rubricata "Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo", estende le disposizioni della legge n. 71/17 relativa alla tutela dei minori attraverso il contrasto alle forme di cyberbullismo, anche ai fenomeni di bullismo. *(B.P.)*

Il testo della legge è consultabile al seguente link

2. **Legge n. 90 del 28 giugno 2024. Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici**

La legge n. 90/2024 introduce nuove disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche dati in uso presso gli uffici giudiziari. Vengono introdotte delle modifiche al codice penale in tema di reati informartici, consistenti in un inasprimento delle pene e nell'introduzione di circostanze aggravanti rispetto alle fattispecie incriminatrici già esistenti e prevedendo, altresì, delle nuove ipotesi delittuose, come il nuovo comma 3 dell'art. 629 c.p. che punisce la realizzazione dell'estorsione mediante la commissione di un reato informatico. *(Li. Pe.)*

Il testo della legge è consultabile al seguente link

3. **Dlgs. n. 138 del 4 settembre 2024. Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148**

Come noto, la direttiva (UE) 2022/2555 c.d. NIS 2, muovendo dal presupposto che «*la rapida trasformazione digitale e l'interconnessione della società* […] *ha portato a un'espansione del panorama delle minacce informatiche, con nuove sfide che richiedono risposte adeguate, coordinate e innovative in*

tutti gli Stati membri» (cons. n. 3), ha imposto a questi ultimi di adottare strategie nazionali efficaci in materia di cybersicurezza.
Il d.lgs. n. 138/2024 stabilisce in sua attuazione misure volte a garantire un livello più elevato di sicurezza informatica su tutto il territorio italiano, contribuendo così ad incrementare il livello comune di sicurezza nell'Unione europea. *(B.P.)*

Il testo del decreto legislativo è consultabile al seguente link

4. **Dlgs. n. 129 del 5 settembre 2024. Adeguamento della normativa nazionale al regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.**

Il decreto legislativo n. 129/2024 fissa il sistema di vigilanza sugli emittenti specializzati di token collegati ad attività e per i prestatori specializzati di servizi per le cripto-attività, attribuendo, da un lato, alla Consob poteri appositi in ordine alla verifica dell'osservanza delle norme relative alla trasparenza e alla correttezza dei loro comportamenti; dall'altro, alla Banca d'Italia poteri relativi alla verifica della loro stabilità finanziaria e della loro adeguatezza patrimoniale.
Unitamente al regime di vigilanza, il legislatore nazionale prevede al titolo VI, conformemente al regolamento *MiCA*, un doppio regime sanzionatorio, in cui la regola è il ricorso alla sanziona amministrativa, salvo alcune violazioni che sono punite solo penalmente. Relativamente a quest'ultime, il legislatore nazionale introduce un nuovo delitto di abusivismo per gli operatori regolamentati, punito con la reclusione da sei mesi a quattro anni e con la multa da euro 2.066 a euro 10.329. *(R.M.V.)*

Il testo del decreto è consultabile al seguente link

5. **D.d.l. sull'Intelligenza Artificiale**

Dopo l'approvazione governativa in data 23 aprile 2024 dello «*Schema di disegno di legge recante disposizioni e delega al governo in materia di intelligenza artificiale*», il testo comunicato alla Presidenza il 20.05.2024, è ora al vaglio del Senato della Repubblica, quale d.d.l. n. 1146.
Il d.d.l. ha lo scopo di adeguare la normativa nazionale all'AI Act europeo, e tratta di temi chiave come l'applicazione dell'intelligenza artificiale in settori sensibili quali sanità, lavoro e giustizia, senza tralasciare la regolamentazione della governance e i diritti d'autore.
Tuttavia, il 5 novembre 2024, la Commissione europea ha inviato al Governo italiano un parere circostanziato (C (2024) 7814) sul disegno di legge di cui sopra, evidenziando alcuni punti di attrito tra il d.d.l. n. 1146 e il Regolamento europeo sull'Intelligenza Artificiale. *(L.P.)*

Il testo del disegno di legge è consultabile al seguente link
Il parere della Commissione è consultabile al seguente link

NOVITÀ GIURISPRUDENZIALI NAZIONALI ED EUROPEE

1. **Corte Costituzionale sul reato di produzione di materiale pedopornografico**

Con ordinanza del 15 settembre 2023, il Tribunale di Bologna aveva sollevato questione di legittimità costituzionale dell'art. 600 ter c.p. in relazione agli artt. 3 e 27, primo e terzo comma, della Costituzione, denunciando «*la mancata previsione, per il reato di produzione di materiale pornografico mediante l'utilizzazione di minori di anni diciotto, dell'attenuante per i casi di minore gravità*».
Con sentenza n. 91/2024, depositata il 20 maggio 2024, la Corte costituzionale ha concluso per la fondatezza della questione e ha dichiarato «*l'illegittimità costituzionale dell'art. 600-ter, primo comma, numero 1), cod. pen., per violazione degli artt. 3 e 27, primo e terzo comma, Cost., nella parte in cui non prevede, per il reato di produzione di materiale pornografico mediante l'utilizzazione di minori di anni diciotto, che nei casi di*

minore gravità la pena da esso comminata è diminuita in misura non eccedente i due terzi». Nell'occasione, la Corte ha ribadito la necessità di assicurare una valvola di sicurezza, che permetta al giudice di «di graduare e "personalizzare" la pena da irrogare in concreto con riferimento ai casi di minore gravità», così da garantire «*il rispetto del principio della proporzionalità della sanzione in una con la individualizzazione della pena e la sua finalità rieducativa*». *(B.P.)*

Corte cost., sentenza 20 maggio 2024, n. 91

2. Reato di pornografia minorile e circostanze attenuanti

A seguito della sentenza della Corte cost., n. 91/2024 che ha dichiarato l'illegittimità costituzionale dell'art. 600-ter, comma 1, n. 1, c.p., nella parte in cui non prevede, per il reato di produzione di materiale pornografico mediante l'utilizzazione di minori di anni diciotto, che nei casi di minore gravità la pena comminata sia diminuita in misura non eccedente i due terzi, s'impone, nel caso di mancato riconoscimento dell'attenuante, una rivalutazione della condotta al fine di riconoscere o meno la sussistenza di tale circostanza (*supra* 1). *(B.P.)*

Cassazione Penale, Sez. III, 13 settembre 2024, n. 34588

3. Pornografia non consensuale quando l'autore della diffusione è diverso da chi ha realizzato il materiale sessualmente esplicito

Il cd. revenge porn presuppone la consapevolezza ed il consenso alla produzione di materiale sessualmente esplicito da parte della persona offesa, tuttavia destinato a rimanere privato: punibile è la fuoriuscita del materiale dall'originario perimetro relazionale privato in assenza di consenso.
L'autore di una delle condotte di diffusione del materiale a contenuto sessualmente esplicito non può che essere il soggetto che ha realizzato il materiale stesso, oppure colui che lo ha sottratto.
In altri termini: sebbene non risulti necessario che le immagini a contenuto sessualmente esplicito siano state realizzate in un contesto relazionale sentimentale stabile, successivamente interrotto, con correlata volontà di rivalsa da parte del soggetto agente, ciò nondimeno l'autore della condotta deve essere colui che aveva in precedenza realizzato il detto materiale, o se ne era impossessato sottraendolo. *(B.P.)*

Cassazione Penale, Sez. V, 20 giugno 2024, n. 24379

4. I confini della prova documentale

«*In tema di mezzi di prova, i messaggi di posta elettronica, i messaggi WhatsApp e gli SMS conservati nella memoria di un dispositivo elettronico conservano la natura di corrispondenza anche dopo la ricezione da parte del destinatario, almeno fino a quando, per il decorso del tempo o per altra causa, essi non abbiano perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento "storico", sicché - fino a quel momento - la loro acquisizione deve avvenire secondo le forme previste dall'art. 254 c.p.p. per il sequestro della corrispondenza*». *(B.P.)*

Cassazione Penale, Sez. II, 28 giugno 2024, n. 25549

5. Stalking online

Il delitto di atti persecutori di cui all'art. 612-bis c.p. può essere integrato dalla pubblicazione reiterata di contenuti minatori o molesti su un profilo di un social network, anche se la persona offesa non è direttamente destinataria dei contenuti stessi, purché l'autore agisca nella ragionevole convinzione che la vittima venga informata, configurando così il dolo generico richiesto dal reato. L'elemento soggettivo del delitto di atti persecutori è infatti integrato dal dolo generico, che richiede la volontà di porre in essere più condotte di minaccia o molestia, avendo consapevolezza della loro idoneità a produrre uno degli eventi previsti dalla norma incriminatrice e dell'abitualità del proprio agire, senza necessità di preordinazione delle condotte. Nel

contesto del delitto di atti persecutori, la consapevolezza dell'agente che i propri messaggi molesti pubblicati su un profilo social siano conoscibili dalla vittima, anche tramite altri soggetti legati da un rapporto qualificato di vicinanza, è quindi sufficiente per integrare la fattispecie criminosa, indipendentemente dall'accesso diretto della vittima ai contenuti. *(B.P.)*

Cassazione Penale, Sez. V, 6 settembre 2024, n. 33986

6. Il reato di illecito trattamento dei dati personali quale reato istantaneo d'evento

Il trattamento illecito di dati (di cui all'art. 167 del Codice Privacy) ha natura di reato istantaneo, in quanto esso si perfeziona con il verificarsi del "nocumento" – da intendersi come un pregiudizio giuridicamente rilevante di qualsiasi natura, patrimoniale o non patrimoniale, conseguenza dell'illecito trattamento – che, per la sua omogeneità rispetto all'interesse leso e la sua diretta derivazione causale dalla condotta tipica è elemento costitutivo del fatto e non condizione oggettiva di punibilità; di conseguenza, il verificarsi dell'evento segna la consumazione del reato. *(B.P.)*

Cassazione Penale, Sez. III, 21 ottobre 2024, n. 38511

7. L'esercizio del diritto di difesa non scrimina una condotta di accesso abusivo ad un sistema informatico protetto

In tema di cause di giustificazione, se è vero che in linea generale il diritto che scrimina ex art. 51, c.p. è quello che, quale che sia la sua collocazione tra le situazioni giuridiche soggettive (diritto, diritto potestativo, potestà, facoltà), attribuisce al soggetto il potere di agire per la sua soddisfazione, sacrificando gli altri interessi con esso contrastanti (si pensi, ad esempio, al diritto di proprietà che consente al titolare di escludere gli altri dal godimento del bene), è altrettanto vero che, allorquando il sacrificio dell'altrui interesse si risolve nella integrazione di una fattispecie penale, che esula dalla tipicità del diritto (nel caso di specie, diritto di difesa), ai fini della giustificazione necessitano determinati stringenti presupposti, non ricomprendendo il diritto di difesa la facoltà di introdursi nel sistema informatico altrui. *(Li.Pe)*

Cassazione Penale, Sez. V, 12 settembre 2024, n. 34501

8. Lo stalking non assorbe il delitto di revenge porn

Il reato di *stalkig* (art. 612-bis c.p.) non assorbe il reato di *revenge porn* (art. 612-ter c.p.). I due reati differiscono per le condotte incriminate, gli eventi richiesti, e la tutela dei beni giuridici, e pertanto concorrono tra loro anche quando le condotte di *revenge porn* incidono sulla libertà morale della vittima. *(Li.Pe)*

Cassazione Penale, Sez. I, 28 agosto 2024, n. 33230

9. La diffamazione attraverso Whatsapp non è aggravvata

Nella pronuncia in esame la Corte di Cassazione esclude la sussistenza della circostanza aggravante di cui al co. 2 dell'art. 227 c.p.m.p. (pressoché identico, nella sua formulazione, al co. 3 dell'art. 595 c.p.: "offesa arrecata con qualsiasi altro mezzo di pubblicità") in un'ipotesi in cui la vittima era stata lesa nel proprio diritto all'onore e alla reputazione all'interno di una chat di whatsapp il cui gruppo era costituito da 156 utenti. *(C.C.)*

Cassazzione Penale, Sez. I, 11 settembre 2024, n. 42783

10. La connessione Internet non rientra nel concetto di energia per cui non può essere applicato il reato di furto

La Corte di legittimità ha ritenuto che la condotta di utilizzo della linea telefonica da parte del dipendente pubblico non potesse rientrare nel paradigma del peculato dell'energia telefonica, in quanto non avente ad oggetto un bene su cui possa manifestarsi una condotta appropriativa, bensì in quello del peculato d'uso dell'apparecchio telefonico. *(C.C.)*

Cassazione Penale, Sez. I, 3 luglio 2024, n. 42127

11. Accesso abusivo a sistema informatico per il superiore gerarchico che utilizza le credenziali di un suo sottoposto

Commette reato di accesso abusivo a sistema informatico ex art. 615-ter cod. pen. il dipendente con poteri direttivi che, pur essendo sovraordinato gerarchicamente al titolare delle credenziali di accesso, se le faccia rivelare da quest'ultimo per accedere al sistema senza specifica autorizzazione. La sola protezione dei dati mediante credenziali d'accesso, imposta dal datore di lavoro, rende implicite e manifeste le direttive aziendali di limitazione e controllo degli accessi. La contestazione, nel capo d'imputazione, di un accesso "per scopi estranei al mandato ricevuto" (accesso disfunzionale) non esclude la sussistenza di un accesso abusivo tout court se dal fatto emerge chiaramente che l'imputato non aveva il diritto di accedere al sistema informatico senza le proprie credenziali. La indeterminatezza o contraddittorietà della contestazione circa la legittimità dell'accesso al sistema informatico, non eccepita nei termini di cui all'art. 491 cod. proc. pen., non determina nullità della sentenza se dal procedimento risulta evidente che l'imputato fosse conscio della carenza di legittimazione all'accesso. *(C.C.)*

Cassazione penale, Sez. V, 8 maggio 2024, n. 40295

NOVITÀ RILEVANTI A LIVELLO NAZIONALE

1. Report Clusit ottobre 2024

Il Rapporto inizia con una panoramica degli incidenti di sicurezza informatica più significativi avvenuti a livello globale (Italia inclusa) nel primo semestre del 2024, confrontandoli con i dati raccolti negli anni precedenti. L'analisi degli attacchi in Italia è poi completata dalle rilevazioni e segnalazioni della Polizia Postale e per la Sicurezza Cibernetica, che ci hanno fornito dati e informazioni estremamente interessanti su attività ed operazioni svolte nel corso dei primi sei mesi di quest'anno. *(B.P.)*

Il report è reperibile al seguente link

2. Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale

Assosoftware, Associazione italiana dei produttori di software in Italia, ha ottenuto l'approvazione del Garante per la protezione dei dati personali per l'adozione di un Codice di condotta che introduce una serie di regole e misure tecniche ed organizzative relative al trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione dei software gestionali (SWH). *(L.P.)*

Il testo del Codice è disponibile al seguente link

VOLUMI E CONTRIBUTI DOTTRINALI DI RILIEVO

Altalex

FILIPPI L., *Le SS.UU. sui criptofonini: ma l'"equo processo" ammette la prova a genesi ignota?,* in I*l quotidiano giuridico*, *3/2024*

LOMBARDO M., *In vigore la Direttiva sulla lotta alla violenza contro le donne e alla violenza domestica*, in *Altalex, 13/06/2024*

Archivio Penale

ANDREUCCIOLI C. (a cura di), *Legge n.90 del 2024- Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (G.U.2.07.2024).*

Diritto di Internet

MARAFRIOTI L., *Tirannie tecnologiche a Sezioni Unite: dati digitali criptati, diritto di difesa e contraddittorio*, n. 4, 2024, p. 729 ss.

PICOTTI L., *Sanità digitale ed Intelligenza Artificiale: profili penali*, n. 3, 2024, p. 415 ss.

TARANTINO S., *Accesso abusivo a sistema informatico di interesse pubblico: il punto della Cassazione sul caso del P.R.A*, n. 3, 2024, p. 527 ss.

TRIPODI E. M., *AI Act e GDPR. Assonanze e dissonanze*, n. 4, 2024, p. 617 ss.

ZARRA P., *L'utilizzo illecito del Jammer per ostacolare le comunicazioni radio tra volante e sala operativa configura il reato di cui all'art. 617-bis c.p.*, n. 4, 2024, p. 753.

Diritto penale e processo

ALBANESE D., *La "nuova" corrispondenza nel processo penale, tra recenti sviluppi giurisprudenziali e scenari de lege ferenda*, 2024, n. 11, p. 1517 ss.

BARONE G., *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti",* 2024, n. 8, p. 991 ss.

ROCCHI F. (a cura di), *Osservatorio Corte di Cassazione - Diritto Penale*, 2024, n. 11, p. 1443 ss.

Discrimen

KOSTORIS R. E., *Intelligenza artificiale, strumenti predittivi e processo penale,* 3/2024

Giurisprudenza penale

CRAVIOTTO A., VITALI L., EGITTO L., CANEPA C., *Per un uso responsabile dell'intelligenza artificiale nel processo (penale),* fasc. 3, 2024.

La legislazione penale

CANATO M., *Verso il superamento del "legal risk" europeo: intelligenza artificiale e approccio proporzionale al rischio*, n. 3, 2024, p. 79 ss.

MALINO E., *Esercizio dell'azione penale e prognosi di condanna mediante software predittivi. Verso la creazione di un pm-robot,* n. 3, 2024, p. 284 ss.

NISCO A., *Le neurotecnologie assistite dall'intelligenza artificiale nell'ottica del diritto penale*, n. 3, 2024, p. 442 ss.

PIETROCARLO E., *La predictive policing nel regolamento europeo sull'intelligenza artificiale*, n. 3, 2024, p. 337 ss.

Rivista Italiana di Diritto e Procedura Penale

CAMALDO L., *Intelligenza artificiale e investigazione penale predittiva*, n. 1, 2024, p. 233 ss

CANESCHI G., *Intelligenza artificiale e sistema penitenziario*, n. 1, 2024, p. 251 ss.

FRAGASSO B., *Intelligenza artificiale e crisi del diritto penale d'evento: profili di responsabilità penale del produttore di sistemi di I.A.,* n. 1, 2024, p. 287 ss.

VASTA V., *Diritto dell'Unione europea e intelligenza artificiale. Riflessi sul procedimento penale*, n. 1, 2024, p. 271 ss.

Sistema Penale

BIANCHI M., *L'abuso dell'immagine intima nella Direttiva (UE) 2024/1385*, 8 novembre 2024

PICOTTI L., *Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palingenesi? Le raccomandazioni dell'*Association Internationale de Droit Pénal *e la rilevanza del recente regolamento europeo sull'intelligenza artificiale*, in *Sistema penale*, 31.7.2024.

Revue Internationale de Droit Pénal (RIDP)

PICOTTI L., PANATTONI B. (ed.), *Traditional Criminal Law Categories and AI: Crisis or Palingenesis?, (International Colloquium Section I*, Siracusa, 15-16 September 2022), Vol. 94 issue 1, 2023.

MIRÒ-LLINARES F., DUVAC C., TOADER T., GALARZA M. S. (ed.), *Criminalisation of AI-related offences*, (*International Colloquium*, Bucharest, Romania, 14-16 June 2023), Vol. 95, issue 1, 2024.

VERMEULEN G., PERSAK N., DE COENSEL S., *Researching the boundaries of sexual integrity, gender violence and image-based abuse*, Vol. 95, issue 2, 2024.

Volumi

CALETTI G., SUMMERER K., *Criminalizing Intimate Image Abuse. A Comparative Perspective*, Oxford University Press, 2024

CRESCIOLI C., *Cybercrime e tutela penale del patrimonio. Un'indagine in prospettiva comparata. Con presentazione del prof. Lorenzo Picotti*, Milano, Giuffrè Francis Lefebvre, 2024.

FIORINELLI G., *La violenza mediata dalla tecnologia. Dogmatica, profili politico-criminali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digitali*, Giappichelli, 2024.

SAVIANO F., *Manuale CISO Security Manager. Manuale per l'attività di CISO / Security Manager basato sulla preparazione per l'esame CISSP, Vol. I - Basi di Sicurezza, Business Continuity, Asset Managment, Normative e Cittografia Teorica,* 2024.

PEROBELLO L., *Il fenomeno dei "deepfake" e le sue implicazioni sul piano penale*, Tesi di Laurea Magistrale in Giurisprudenza, Università degli Studi di Verona, 2024.

Convegni:

STATI GENERALI DEL DIRITTO DI INTERNET E DELL'INTELLIGENZA ARTIFICIALE – IV edizione a cura dei proff. Francesco Di Ciommo e Giuseppe Cassano, LUISS 28, 29, 30 novembre 2024.
https://dirittodiinternet.it/stati-generali-del-diritto-di-internet-e-della-intelligenza-artificiale-iv-edizione/