Cybercrime: rassegna delle novità (aprile – agosto 2023)

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

Responsabili scientifici: Prof. Lorenzo Picotti e Prof. Luca Lupária - monitoraggio e redazione a cura di Alice Baccin, Marco Mattia e Marco Pittiruti

NOVITÀ SOVRANAZIONALI

1. Proposta di Regolamento del Parlamento Europeo e del Consiglio di modifica del Regolamento UE 2019/881 per quanto riguarda i servizi di sicurezza gestiti – COM(2023) 208 final

In data 18 aprile 2023 è stata pubblicata la proposta di Regolamento europeo tesa a modificare il testo dell'attuale Regolamento (EU) 2019/881 in materia di *cybersecurity* (cd. *Cybersecurity Act*) con il fine di consentire, mediante atti esecutivi della Commissione, l'adozione di sistemi europei di certificazione dei servizi di sicurezza gestiti, in aggiunta a quelli già esistenti in materia di prodotti informatici tecnologici (TIC), servizi e processi tecnologici.

Nella proposta, il legislatore europeo manifesta, infatti, la volontà di non intervenire sulle caratteristiche e sul funzionamento del *Cybersecurity Act*, spiegando di voler migliorare la qualità e la comparabilità dei sistemi di sicurezza gestiti in linea con quanto previsto dall'intero *corpus* normativo esistente in materia di *cybersecurity*, e con la legge europea sulla solidarietà informatica (*EU Cyber Solidarity Act*) di cui si parlerà *infra* (A.B.) (M.M.)

[Proposal for a Regulation of the European Parliament and of the Council amending Regulation \(EU\) 2019/881 as regards managed security services COM\(2023\) 208 final](#)

2. EU Cyber Solidarity Act: avanzata dalla Commissione Europea la proposta di legge sulla solidarietà informatica per migliorare la preparazione, l'individuazione e la risposta agli incidenti di cybersicurezza in tutta l'Unione Europea – COM (2023) 209 final

Sempre in data 18 aprile 2023, la Commissione Europea ha pubblicato una proposta di Regolamento sulla solidarietà informatica (*Cyber Solidarity Act*), la quale mira a rafforzare la capacità dell'Unione Europea di individuare, preparare e rispondere a minacce e attacchi significativi/su larga scala in materia di cybersicurezza. La proposta di legge prevede l'introduzione di uno scudo europeo per il cyberspazio (*European Cyber Shield*) composto da tanti centri operativi per la sicurezza (denominati SOC) sparsi in tutta Europa, con compiti di *detection* e risposta delle minacce informatiche: i primi tre SOC – centri operativi di sicurezza transfrontalieri – sono già stati individuati nel novembre 2022 in seno al programma Europa Digitale e riuniscono organismi di diciassette Stati membri e Islanda. A ciò si aggiungano (i) la previsione di attività di *testing* della sicurezza informatica in settori cruciali come finanza, energia e assistenza sanitaria, (ii) la creazione di una riserva europea per la cybersicurezza – intesa quale servizio di risposta immediata agli incidenti informatici erogato da servizi privati (cd. fornitori di fiducia) a supporto di Stati membri, istituzioni, organi o agenzie vittime di incidenti di cybersicurezza – e (iii) l'assistenza reciproca tra Stati qualora uno dei membri si trovi esposto ad attacchi. Da ultimo, la proposta prevede anche l'istituzione di un meccanismo di revisione degli incidenti di cybersicurezza con lo scopo di rivalutare e investigare su specifici incidenti potenzialmente sospetti, anche raccogliendo insegnamenti e raccomandazioni utili per migliorare la risposta informatica dell'Unione (A.B.) (M.M.)

[Proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare and respond to cybersecurity threads and incidents COM\(2023\) 209 final](#)

3. Corte Europea dei Diritti Umani, Grande Camera, 15 maggio 2023, Sanchez c. Francia - Contenuti discriminatori, hate speech e obbligo di cancellare i commenti online

La Corte EDU torna a pronunciarsi in materia di *hate speech*, concentrandosi sull'ipotesi di responsabilità dell'autore di un post in Facebook, per omessa rimozione di commenti offensivi pubblicati da terzi. A seguito del ricorso presentato da un cittadino francese condannato in via definitiva dalle autorità nazionali per incitamento all'odio o alla violenza, infatti, i giudici di Strasburgo hanno escluso che contrasti con l'art. 10 CEDU l'imposizione di una responsabilità vicaria in capo all'autore di un contenuto *online* per contenuti postati da terzi, anche enfatizzando la qualifica di personaggio politico del titolare del profilo. Il ricorrente, infatti, era all'epoca dei fatti sindaco della città di Beaucaire, deputato del Parlamento UE e candidato alle elezioni nazionali, e aveva pubblicato sulla propria bacheca Facebook (aperta al pubblico) un post di critica nei confronti del mancato funzionamento del sito internet di un collega europarlamentare. Dal post erano, poi, scaturite plurime interazioni, tra cui alcuni commenti contenenti frasi offensive nei confronti dell'avversario, mai rimossi. Sottoposto a procedimento penale insieme agli autori dei commenti, il ricorrente veniva condannato al pagamento di una multa e avanzava ricorso dinnanzi ai giudici di Strasburgo per violazione della libertà di espressione garantita dall'art. 10 CEDU, condanna confermata dalla Corte che ha riconosciuto la piena responsabilità del ricorrente pur in presenza di commenti attribuibili ad altri e constatato l'assenza di qualsiasi violazione della libertà di espressione pur alla luce del suo ruolo pubblico, del contesto sociale già "infiammato" presente all'epoca dei fatti, e delle successive interazioni generate dai commenti (A.B.).

[Corte Europea dei Diritti Umani, Grande Camera, 15 maggio 2023, n. 45581/23 – Sanchez c. Francia](#)

4. Corte di Giustizia dell'Unione Europea – Comunicato stampa n. 98/23 del 8.6.2023 – Conclusioni dell'Avvocato Generale Szpunar nella causa C 376/22 (Google Ireland e a.): a piattaforme come Google, Meta Platforms e Tik Tok possono essere imposti obblighi supplementari in uno Stato membro diverso da quello della loro sede solo mediante provvedimenti adottati caso per caso

Google, Meta Platforms e Tik Tok contestavano dinanzi ai giudici austriaci la constatazione meramente dichiarativa dell'autorità austriaca di regolazione delle comunicazioni (KommAustria), secondo la quale la legge federale austriaca del 2020, recante misure di protezione degli utilizzatori delle piattaforme di comunicazione (KoPl-G1), sarebbe applicabile nei loro confronti, sebbene esse siano stabilite in un altro Stato membro, ossia l'Irlanda. Tale legge mira a rafforzare la responsabilità delle piattaforme di comunicazione, obbligando in maniera generale i fornitori di «piattaforme di comunicazione», con sede in Austria o all'estero, a istituire un sistema di notifica e di verifica dei contenuti potenzialmente illeciti. Gli obblighi derivanti dal KoPl-G1 non esigono che sia stato previamente adottato un provvedimento individuale e specifico. Peraltro, tale legge stabilisce ammende in caso di violazione degli obblighi da essa derivanti.

Google, Meta Platforms e Tik Tok sostenevano l'incompatibilità del KoPl-G1 con la direttiva sul commercio elettronico del 8.6.2000, in particolare con il "principio del paese d'origine". La Corte amministrativa austriaca sottoponeva alla Corte di giustizia talune questioni al riguardo, in particolare chiedendo se uno Stato membro possa legittimamente limitare la libera circolazione dei servizi della società dell'informazione provenienti da altri Stati membri adottando provvedimenti legislativi di carattere generale e astratto riguardanti una data categoria di servizi della società dell'informazione, descritta in termini generali come «piattaforme di comunicazione», senza che tali provvedimenti siano adottati caso per caso indicando nominativamente le piattaforme designate.

Nelle sue conclusioni, l'avvocato generale Maciej Szpunar, muovendo dall'assunto che i servizi forniti in Austria dalle tre società di cui trattasi costituiscono servizi della società dell'informazione, come sostenuto dalla Corte amministrativa austriaca, ha evidenziato che - nell'ambito regolamentato - la direttiva sul commercio elettronico vieta agli Stati membri di limitare la libera circolazione dei servizi della società dell'informazione provenienti da un altro Stato membro. La suddetta direttiva osta in linea di principio, fatte salve le deroghe, a che il prestatore di un servizio del commercio elettronico sia soggetto a prescrizioni più rigorose di quelle previste nell'ordinamento del suo Stato d'origine.

Quanto alle deroghe al principio del paese d'origine previste dalla direttiva, l'avvocato generale ha ribadito le sue conclusioni presentate nella causa Airbnb Ireland: a suo avviso, uno Stato membro diverso da quello d'origine può derogare alla libera circolazione dei servizi della società dell'informazione solo mediante provvedimenti adottati «caso per caso», previa notifica alla Commissione, e chiedere allo Stato membro d'origine di adottare provvedimenti in materia di servizi della società dell'informazione, il che non si verificava

nel caso di specie. Peraltro, il fatto di considerare che una disposizione generale e astratta che si applica a qualsiasi prestatore di una categoria dei servizi della società dell'informazione costituisca un «provvedimento» equivarrebbe ad autorizzare la frammentazione del mercato interno mediante normative nazionali. Inoltre, autorizzare l'applicazione di leggi diverse a un prestatore sarebbe in contrasto con l'obiettivo, perseguito dalla direttiva, di sopprimere gli ostacoli giuridici al buon funzionamento del mercato interno. Pertanto, l'avvocato generale ha evidenziato come la suddetta direttiva osti a che uno Stato membro possa limitare, in circostanze siffatte e in tal modo, la libera circolazione dei servizi della società dell'informazione provenienti da un altro Stato membro. (M.M.)

<https://curia.europa.eu/juris/documents.jsf?num=C-376/22>

4. INTERPOL e UNICRI pubblicano un progetto per un uso responsabile dell'IA da parte delle forze dell'ordine. Il toolkit AI fornisce una guida strategica e pratica per dirigenti e agenti di polizia (Singapore - giovedì 8 giugno 2023)

Mentre l'intelligenza artificiale (AI) continua a diffondersi all'interno dei più disparati campi dell'esperienza, rivoluzionando il modo in cui funzionano ampi settori della società, è sempre più chiaro che coloro che cercheranno di sfruttarne il potenziale dovranno farlo all'interno di un quadro prestabilito. L'uso di questa tecnologia da parte delle forze dell'ordine non fa eccezione.

Assieme ai rappresentanti della comunità globale delle forze dell'ordine riuniti per il Congresso sulla scienza della polizia dell'INTERPOL a Singapore, l'INTERPOL e l'Istituto interregionale di ricerca sul crimine e la giustizia delle Nazioni Unite (UNICRI) hanno presentato, in data 8 giugno 2023, il loro *Toolkit for Responsible AI Innovation in Law Enforcement*: una guida pratica per le forze dell'ordine sullo sviluppo e la diffusione responsabile dell'intelligenza artificiale, nel rispetto dei diritti umani e dei principi etici.

Sviluppato congiuntamente dal Centro per l'intelligenza artificiale e la robotica dell'UNICRI e dal Responsible AI Lab dell'INTERPOL, con il sostegno finanziario dell'Unione Europea, l'AI Toolkit è la risposta a una corale richiesta da parte delle forze dell'ordine di una guida nell'utilizzo dell'intelligenza artificiale.

In effetti, le forze dell'ordine stanno già facendo ampio uso di sistemi di intelligenza artificiale, o di sistemi con componenti di intelligenza artificiale, ma molti di questi strumenti potrebbero non essere stati prodotti allo specifico fine di coadiuvare le attività di polizia.

Riflettendo su questo, il segretario generale dell'INTERPOL Jürgen Stock ha dichiarato: “*L'intelligenza artificiale rappresenta innegabilmente un punto di svolta sia per i criminali che per le forze dell'ordine. Tuttavia, è imperativo effettuare il passaggio alla nuova era tecnologica in modo affidabile, legale e responsabile, fornendo un modo chiaro, pragmatico e soprattutto utile*”.

L'AI Toolkit, che comprende sette risorse distinte, supportate da una guida utente completa, fornisce indicazioni ai dirigenti e ai funzionari delle forze dell'ordine per orientarsi nell'innovazione responsabile dell'IA, tra cui: i fondamenti tecnici dell'IA; principi guida per un uso responsabile, in linea con i principi di polizia; valutazioni organizzative sulla prontezza e sul rischio.

Concepito come uno strumento in evoluzione, il toolkit per l'intelligenza artificiale sarà aggiornato e rivisto regolarmente per garantire che le forze dell'ordine possano tenere il passo con i rapidi sviluppi in questo campo e con le sfide legali ed etiche ad esso associate. Questo percorso sarà integrato da iniziative di rafforzamento delle capacità e dal sostegno ai paesi che desiderano elaborare linee guida o strategie nazionali.

In definitiva, le autorità nazionali mantengono la piena autonomia nel loro percorso verso l'IA. L'AI Toolkit aiuterà i policymakers delle forze dell'ordine a orientarsi nei dibattiti e nelle discussioni che costituiscono parte integrante di questo processo. (M.M.)

<https://unicri.it/News/UNICRI-INTERPOL-release-Toolkit-for-Responsible-AI-Innovation-Law%20-Enforcement>

5. Il Parlamento Europeo approva la posizione negoziale sulla legge in materia di intelligenza artificiale (Artificial Intelligence Act): al via i colloqui con i governi degli Stati membri

Il 14 giugno 2023, il Parlamento europeo ha votato con 499 voti favorevoli, 28 contrari e 93 astensioni la posizione negoziale relativa alla legge sull'Intelligenza artificiale, di fatto sancendo l'inizio dei colloqui con i governi degli Stati membri in relazione al testo definitivo. Si tratta della prima regolamentazione esaustiva e

uniforme in materia al mondo, la cui approvazione definitiva dovrebbe arrivare entro fine anno per entrare in vigore tra il 2024 e il 2025. Dal punto di vista strettamente giuridico, infatti, l'*AI Act* punterà a regolamentare lo sviluppo, la commercializzazione e l'uso dei sistemi di IA, anche aprendo la strada all'utilizzo su vasta scala dei cd. modelli di intelligenza artificiale generativa (quali Chat GPT e Bard).

Con il proprio voto, il Parlamento si è altresì espresso a favore del divieto di categorizzazione biometrica sulla base di caratteristiche sensibili (identità sessuale, razza, genere, etnia), del riconoscimento delle emozioni nei contesti educativi, nei luoghi di lavoro e da parte della polizia (interna e transfrontaliera) e sui rischi correlati alla capacità dei sistemi dotati di intelligenza artificiale di influenzare gli elettori nel corso delle tornate elettorali, sicché la posizione di giugno si configura quale ultimo e più recente passo nel quadro dell'approccio europeo all'intelligenza artificiale, sancendone il ruolo di *leader* mondiale nella regolamentazione del settore tecnologico (A.B.)

[Intelligenza artificiale: deputati pronti a negoziare le prime norme per un'IA sicura e trasparente](#)

6. Pubblicato da Europol il nuovo Internet Organised Crime Assessment (IOCTA) 2023 contenente la valutazione sulle minacce legate alla criminalità organizzata informatica

Europol ha pubblicato in data 17 luglio 2023 il nuovo *report* IOCTA contenente la nona valutazione relativa alle minacce della criminalità organizzata su Internet, la quale ha evidenziato come i fenomeni di *hacking* rappresentino, oggi, un vero e proprio ecosistema criminale radicato. Le principali forme di criminalità informatica si concretizzano, infatti, sotto forma di attacchi informatici, frodi *online* e sfruttamento sessuale *online* dei minori, avendo l'*hacking* smesso di essere un fenomeno isolato per diventare un vero e proprio *business* globale. Le diverse associazioni di criminali informatici, peraltro, mettono a fattor comune conoscenze e competenze, concorrendo alla realizzazione degli attacchi informatici e avvalendosi, ai fini dell'anonimato, della struttura del *deep web*, per un giro complessivo d'affari su base multinazionale cui partecipano diversi fiancheggiatori e finanziatori. In linea con quanto emerso dal *report* IOCTA, Europol ha annunciato, sempre in data 17 luglio 2023, la pubblicazione di alcuni *spotlight report* relativi ai cyber attacchi, alle frodi *online* e allo sfruttamento dei minori *online*, i quali verranno resi noti prossimamente (A.B.) (M.M.).

[Internet Organised Crime Assessment \(IOCTA\) 2023](#)

7. In vigore il Data Privacy Network per il trasferimento di dati tra USA e Europa

Il 10 luglio 2023 la Commissione Europea ha adottato la decisione di adeguatezza sul EU-US Data Privacy Network re-inserendo gli Stati Uniti nell'elenco dei paesi che garantiscono un livello di protezione adeguato ai dati trasferiti dall'Unione Europea verso le società statunitensi che aderiscono al quadro comune sulla *privacy*. La decisione di adeguatezza fa seguito alla firma, in data 7 ottobre 2022, dell'Executive Order 14086 da parte del presidente Biden il quale ha introdotto, unitamente ad altri regolamenti previamente adottati, una serie di garanzie a tutela dei dati inviati dai cittadini europei, tra cui (i) garanzie vincolanti che limitano l'accesso dei dati da parte delle autorità di *intelligence* statunitensi se non nei casi in cui detto accesso risulti necessario per la tutela della sicurezza nazionale, (ii) una maggiore supervisione delle attività dei servizi di *intelligence* al fine di garantire il rispetto di dette limitazioni, (iii) l'istituzione di un meccanismo di ricorso indipendente e imparziale – un tribunale specifico – competente in relazione ai reclami avanzati da cittadini UE a fronte dell'accesso indebito da parte delle autorità di sicurezza nazionali statunitensi ai propri dati.

Obiettivo della decisione è prevenire trattamenti illeciti e indebite forme di ingerenza sui dati che provengono dall'Unione Europea, in linea con quanto già previsto dalla normativa interna racchiusa nel GDPR, assicurando nel contempo con tali regole la possibilità di trasferimento di dati da Stati dell'Unione europea (A.B.).

[Decisione di adeguatezza sul EU-US Data Privacy Network](#)

8. Ethics in the Age of Disruptive Technologies: anche il Vaticano adotta un manuale etico sull'intelligenza artificiale

Anche la Santa Sede interviene sul dibattito esistente in merito all'uso etico dell'intelligenza artificiale pubblicando un proprio manuale etico denominato *Ethics in the Age of Disruptive Technologies: An Operational Roadmap* in collaborazione con l'Università statunitense di Santa Clara. L'iniziativa, diffusa nel

giugno 2023, è stata, infatti, guidata congiuntamente dall'Institute for Technology, Ethics and Culture (ITEC) della Santa Clara University e dal Dicasterium de Cultura et Educatione del Vaticano, ponendosi quale obiettivo quello di indirizzare la discussione circa i profili di etica, sostenibilità e gestione dell'intelligenza artificiale, senza tuttavia esprimersi sui profili legali della questione. Già dalle prime pagine, infatti, il manuale sottolinea di non voler riscrivere o sostituire il *framework* legale esistente, limitandosi a riflessioni di natura squisitamente etica anche con riferimento alle zone grigie dell'AI quali crittografia e riconoscimento biometrico (A.B.).

[*Ethics in the Age of Disruptive Technologies: An Operational Roadmap*](#)

9. Approvato il Regolamento europeo sui microchip (Chips Act) che istituisce un quadro di misure europee per rafforzare l'ecosistema europeo dei semiconduttori – COM(2022) 46 final

Il 25 luglio 2023 il Consiglio dell'Unione Europea ha approvato definitivamente il cd. *Chips Act*, il Regolamento in materia di semiconduttori predisposto dal legislatore comunitario nel tentativo rafforzare il sistema europeo di approvvigionamento dei semiconduttori utili alla produzione di dispositivi elettronici e di ridurre la dipendenza da attori economici esterni quali Cina, Taiwan, Corea del Sud, Giappone e Stati Uniti.

In particolare, il Regolamento mira a (i) sviluppare una base industriale europea nel settore dei microchip, (ii) attrarre investimenti, (iii) promuovere la ricerca e l'innovazione nel campo anche al fine di scongiurare eventuali crisi dovute alla mancanza di semiconduttori in futuro.

In quest'ottica, il *Chips Act* stanziava investimenti per circa quarantatré miliardi di Euro sia nel settore pubblico, che nel settore privato, con l'obiettivo di accrescere la quota UE nel mercato dei semiconduttori dall'attuale 10% ad almeno il 20% entro il 2030 (A.B.) (M.M.)

[Proposta di Regolamento del Parlamento Europeo e del Consiglio che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori \(normativa sui chip\) COM\(2022\) 46 final](#)

10. Prove elettroniche e procedimento penale: pubblicati il Regolamento (UE) 2023/1543 del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali e la Direttiva (UE) 2023/544 recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali

Nel quadro della cooperazione giudiziaria e di polizia in materia penale, il Parlamento Europeo e il Consiglio hanno pubblicato, in data 28 luglio 2023, il Regolamento (UE) 2023/1543 relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali, il quale stabilisce le norme in base alle quali un'autorità di uno Stato membro può, nell'ambito di un procedimento penale, emettere un ordine europeo di produzione o un ordine europeo di conservazione e ingiungere a un prestatore di servizi interno all'UE di produrre o conservare prove elettroniche indipendentemente dall'ubicazione dei dati. Tale Regolamento fa il paio, inoltre, con la Direttiva (UE) 2023/544 emanata sempre in data 28 luglio 2023, che definisce norme sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali di determinati prestatori di servizi che offrono servizi nell'Unione ai fini della ricezione, dell'ottemperanza e dell'esecuzione di decisioni e ordini emessi dalle autorità competenti degli Stati membri per acquisire le prove nei procedimenti penali (A.B.) (M.M.)

[Regolamento \(UE\) 2023/1543 del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali](#)

[Direttiva \(UE\) 2023/544 recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali](#)

11. Rapporto EFEC del 11 settembre 2023 (di imminente pubblicazione) sulla criminalità economica e finanziaria

Come recentemente segnalato da Europol sul suo sito istituzionale, risulta di imminente pubblicazione (presumibilmente in data 11 settembre 2023) un interessante report a cura del *European Financial and Economic Crime Threat Assessment* (EFECC) sulle minacce attuali ed emergenti legate alla criminalità finanziaria ed economica.

Più in particolare, utilizzando insights ed esempi di casi tratti dal centro anticrimine dedicato di Europol, il rapporto analizzerà le minacce implicate dal riciclaggio di denaro, dalle finanze criminali e dalla corruzione, e come queste si sono evolute a seguito dei cambiamenti tecnologici e geopolitici. Il rapporto esaminerà inoltre il ruolo di questi crimini nel quadro più ampio della criminalità organizzata a livello internazionale, in cui le reti criminali utilizzano la criminalità finanziaria ed economica come strumento per oscurare e, in ultima analisi, trarre vantaggio dai profitti realizzati da attività illegali.

In chiave più strettamente penalistica (ad es. al fine di cogliere eventuali nuovi “segnali d’allarme” rispetto al frenetico evolversi delle complesse fenomenologie criminali in oggetto, evidenziando conseguentemente nuove possibili sfumature di offensività sottese alle stesse) sarà dunque importante valorizzare i risultati della ricerca in oggetto, anche considerando la particolare modalità d’indagine impiegata da Europol, che risulta calibrata su risultanze criminologiche di carattere squisitamente empirico. (M.M.)

[News relativa alla prossima uscita del rapporto EFECC](#)

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Il Garante della Privacy interviene in relazione al delicato rapporto tra diritto di cronaca e tutela della privacy: costituisce interferenza illecita nella vita privata ai sensi dell’art. 615 bis cod. pen. l’acquisizione mediante fotografie di momenti privati all’interno dell’abitazione

In data 8 giugno 2023 il Garante per la protezione dei dati personali ha sanzionato una testata giornalistica per aver pubblicato scatti fotografici realizzati dall’esterno di una abitazione privata in violazione dei principi generali di trattamento delle regole deontologiche. Nell’evidenziare la necessità di trovare un contemperamento tra diritto di cronaca e tutela della *privacy*, il Garante ha rilevato in questo fatto violazioni in materia di tutela dei dati personali e ha esplicitato la natura (anche) penalmente illecita di una simile condotta, idonea ad integrare il delitto di interferenze illecite nella vita privata di cui all’art. 615 bis cod. pen. (A.B.)

[Autorità Garante per la protezione dei dati personali – provvedimento 8 giugno 2023 \[9907956\]](#)

2. Presentata al Senato una proposta di legge relativa al sequestro dei dispositivi e sistemi informatici, smartphone e memorie digitali (DDL S. 806 – XIX Leg.)

In data 19 luglio 2023 è stata presentata una proposta di legge che propone modifiche al codice di procedura penale con riferimento all’acquisizione di dispositivi e sistemi informatici, smartphone e memorie digitali, e ciò a seguito dell’indagine conoscitiva avviata dalla Commissione Giustizia del Senato lo scorso gennaio sul tema delle intercettazioni. Secondo i proponenti, infatti, anche il sequestro dei menzionati dispositivi dovrebbe essere circondato dalle garanzie processuali previste in materia di intercettazioni, sicché anche la selezione dei contenuti rilevanti dovrebbe essere preceduta da un contraddittorio delle parti per deciderne la rilevanza a fini processuali. A questo scopo, la proposta di legge mira **a inserire nell’impianto codicistico un nuovo** art. 254 *ter* cod. proc. pen. prevedendo che l’Autorità giudiziaria disponga il sequestro dei dispositivi informatici con decreto motivato in cui siano indicate espressamente (i) le ragioni che rendono necessario il sequestro in relazione al nesso di pertinenza tra bene appreso e oggetto delle indagini, (ii) le operazioni tecniche da svolgere sul bene appreso e i criteri utilizzati per apprendere le informazioni necessarie al proseguo delle indagini (A.B.).

[DDL S. 806 – XIX Leg. 19 luglio 2023 – Modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici smartphone e memorie digitali](#)

3. Pubblicato in Gazzetta Ufficiale il decreto legislativo 24 luglio 2023, n. 107 di adeguamento della normativa nazionale alle disposizioni del regolamento (UE)2021/784 del Parlamento Europeo e del Consiglio del 29 aprile 2021 relativo al contrasto della diffusione di contenuti terroristici online

È stato pubblicato in Gazzetta Ufficiale il Decreto Legislativo 24 luglio 2023, n. 107 che ha recepito nell'ordinamento interno il Regolamento (UE)2021/784 relativo al contrasto della diffusione di contenuti terroristici *online*. Il Regolamento, emesso nell'aprile 2021, prevede l'obbligo per le piattaforme internet di dotarsi di misure specifiche di vigilanza rispetto a potenziali contenuti rischiosi, attivandosi nell'immediato per rimuoverli o disabilitarne l'accesso su ordine dell'autorità nazionale competente. Nell'adeguare la normativa interna al corpus comunitario, il legislatore all'art. 7, D.lgs. n. 107/2023, ha previsto a corredo una serie di fattispecie penali, tese a sanzionare molteplici ipotesi di illecito che siano commesse dal prestatore di servizi di *hosting* che (i) non abbia istituito punti di contatto per la ricezione degli ordini di rimozione o ometta di rendere disponibili al pubblico le informazioni relative al punto di contatto; (ii) ometta di designare il rappresentante legale nell'Unione per il ricevimento, l'attuazione e l'esecuzione degli ordini di rimozione o designi un soggetto fuori dall'Unione, (iii) ometta di rimuovere i contenuti terroristici o di disabilitarne l'accesso; (iv) non informi l'autorità giudiziaria della presenza dei contenuti terroristici; (v) ponga in essere violazioni sistematiche e persistenti degli obblighi previsti dalla normativa europea (A.B.) (M.M.).

[Decreto Legislativo 24 luglio 2023, n. 107 di adeguamento della normativa nazionale alle disposizioni del regolamento \(UE\) 2021/784](#)

4. Legge 14 luglio 2023, n. 93 – Disposizione per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica

In data 8 agosto 2023 è entrata in vigore la Legge 14 luglio 2023, n. 93 in materia di prevenzione e repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante reti di comunicazione elettronica, la quale introduce alcune significative novità in materia di diritto penale d'autore incrementando i profili di tutela *online* della proprietà intellettuale e dei relativi soggetti coinvolti. Più nello specifico, la legge si colloca a valle delle discussioni avviate in seno all'Unione Europea con il piano di azione sulla proprietà intellettuale avviato nel 2020, cui ha fatto seguito la pubblicazione di una raccomandazione UE contro la pirateria *online* in data 4 maggio 2023. Tra le novità più rilevanti, oltre alla modifica degli artt. 171 *ter* e 174 *ter* della Legge 633/1941 – che puniscono oggi chiunque esegua la fissazione su supporto digitale, audio, video o audiovisivo di opere cinematografiche, audiovisive o editoriali ovvero ne esegua la riproduzione, l'esecuzione o la comunicazione al pubblico o chi duplichi e metta a disposizione opere o materiali resi accessibili in maniera abusiva mediante supporti digitali, audio, video, audiovisivo – vi è il ruolo preminente dell'AGCOM, che avrà ora il potere di disabilitare i contenuti abusivi tramite il blocco dei nomi di dominio e del traffico di rete e di convocare un tavolo tecnico per consentire la disabilitazione dei domini e indirizzi IP segnalati. Qualora il soggetto bloccato si trovi al di fuori del territorio UE, l'Autorità dovrà inserirne immediatamente il nominativo su una specifica lista denominata *Counterfeit and Privacy Watch List* compilata annualmente dalla Commissione Europea (A.B.).

[Legge 14 luglio 2023, n. 93 in materia di Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica](#)

[Raccomandazione \(UE\) 2023/1018 della Commissione del 4 maggio 2023 sulla lotta alla pirateria online degli eventi sportivi e di altri eventi in diretta](#)

5. AGCOM approva le modifiche al Regolamento sul diritto d'autore online (Delibera n. 680/13/CONS) riguardante il contrasto dell'offerta illegale di contenuti sportivi live.

Il Consiglio dell'Autorità per le Garanzie nelle Comunicazioni, nella seduta del 26 luglio 2023, ha approvato all'unanimità, con Delibera 189/23/CONS, le modifiche al Regolamento sul diritto d'autore online (Delibera n. 680/13/CONS) riguardante il contrasto dell'offerta illegale di contenuti sportivi live. Le nuove disposizioni attribuiscono all'Agcom il potere di emanare le cd. "ingiunzioni dinamiche", sulla scorta di quanto previsto dalla Raccomandazione della Commissione europea sulla lotta alla pirateria online del 4 maggio 2023 (vedi sopra).

Con tali misure, sarà possibile disabilitare l'accesso a contenuti pirata nei primi 30 minuti della trasmissione dell'evento, mediante il blocco della risoluzione DNS dei nomi di dominio e il blocco dell'instradamento del traffico di rete verso gli indirizzi IP univocamente destinati ad attività illecite. Il provvedimento si pone in

linea con la Legge 14 luglio 2023, n. 93, recante Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica, entrato in vigore l'8 agosto (vedi sopra) e grazie alla quale l'Autorità potrà intervenire, con le stesse modalità, per interrompere la diffusione pirata di tutti gli eventi trasmessi in diretta, anche non sportivi. Il Commissario Massimiliano Capitano, relatore del provvedimento, ha così commentato l'iniziativa: *“Con questa modifica, in perfetta sincronia con le novità introdotte dal Parlamento, Agcom si pone ancora una volta all'avanguardia nel panorama europeo nel contrasto all'attività di pirateria on line”*. (M.M.)

[Comunicato stampa AGCOM](#)

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Corruzione di minorenni: sussiste il delitto anche nel caso in cui gli atti siano compiuti a distanza tramite videochat

Il delitto di corruzione di minorenni realizzato mediante il compimento di atti sessuali in presenza di persona infraquattordicenne al fine di farla assistere, di cui all'art. 609- quinquies, comma 1, c.p., è configurabile anche nel caso in cui tali atti, pur compiuti a distanza, siano condivisi con il minore mediante *videochat*, nel corso della loro commissione, posto che il mezzo di comunicazione telematica, volutamente utilizzato dall'agente, consente di ritenere gli atti commessi in presenza della persona offesa (A.B.).

[Corte di Cassazione, Sez. II penale, 12 aprile 2023 \(ud. 23 marzo 2023\), n. 15261](#)

2. Il pedinamento elettronico non viola il diritto alla riservatezza (anche a seguito della riforma in materia di data retention)

Il pedinamento elettronico attraverso sistema di rilevamento satellitare rappresenta un mezzo atipico di ricerca della prova, ricompreso tra i compiti istituzionali di cui la polizia giudiziaria fa legittimo uso, giacché va escluso che tale attività costituisca una interferenza lesiva del diritto alla riservatezza delle comunicazioni ovvero alla inviolabilità del domicilio. A parere dei giudici di legittimità, tali conclusioni non meritano ripensamento alla luce della decisione della Corte di Giustizia dell'Unione Europea del 5 aprile 2022 (C-140/2020) in tema di *data retention* e della riforma di quest'ultima materia ad opera del D.L. n. 132/2021, convertito nella L. n. 178/2021. Invero, l'attività di pedinamento elettronico sarebbe del tutto diversa rispetto alla conservazione di dati, poiché solo quest'ultima porrebbe il problema della tutela del diritto alla riservatezza in ipotesi di massivo accumulo di dati sensibili da parte del gestore del servizio, il che imporrebbe i rigidi limiti teorizzati dalla giurisprudenza europea per l'accesso al dato e alla sua utilizzabilità. (M.P.)

[Corte di Cassazione, Sez. VI penale, 12 aprile 2023 \(ud. 9 marzo 2023\), n. 15422](#)

3. Tabulati telefonici e dati di geolocalizzazione nel giudizio abbreviato: inutilizzabilità dei dati raccolti senza autorizzazione da parte del giudice procedente

Non sono utilizzabili nel giudizio abbreviato i dati di geolocalizzazione relativi a utenze telefoniche o telematiche contenuti in tabulati telefonici acquisiti dalla polizia giudiziaria in assenza del decreto di autorizzazione dell'Autorità giudiziaria in violazione dell'art. 132, co. 3, D.lgs. n. 196/2003, e ciò in quanto trattasi di prove lesive del diritto alla segretezza delle comunicazioni costituzionalmente tutelato e, pertanto, affette da inutilizzabilità patologica, non sanata dalla richiesta di definizione del giudizio con le forme del rito alternativo (A.B.)

[Corte di Cassazione, Sez. VI penale, 14 aprile 2023 \(ud. 11 gennaio 2023\), n. 15836](#)

4. L'utilizzabilità dei messaggi estrapolati dai server di SKY ECC da autorità giudiziaria estera

La sentenza in esame si inserisce nell'ormai cospicuo filone di pronunce chiamate a stabilire l'utilizzabilità dei messaggi estrapolati dai *server* esteri della rete di messaggistica criptata (c.d. criptofonini), ora defunta,

denominata SKY ECC. Nel caso di specie, il pubblico ministero aveva richiesto al Tribunale di Parigi, ai sensi dell'art. 45 del D. Lgs. n. 108/2017 sull'ordine di indagine europeo, l'invio di documentazione relativa alle comunicazioni già autonomamente acquisite da quella autorità giudiziaria sui *server* utilizzati da SKY ECC, documentazione successivamente posta a fondamento di un'ordinanza custodiale. La Suprema Corte ne inferisce che si è trattato di un'acquisizione di dati di tipo "statico", che troverebbe il referente a livello interno nell'art. 234-*bis* c.p.p. A parere dei giudici di legittimità, il requisito relativo al consenso del legittimo titolare sarebbe stato rispettato, provenendo i dati da soggetto – l'autorità giudiziaria francese – che poteva validamente disporre, trattandosi di attività acquisitiva svolta sotto la direzione di un giudice. Quanto al contenuto delle comunicazioni, la censura difensiva volta a contestare le attività tecniche compiute per la decrittazione dei messaggi è stata rigettata argomentando che, per un verso, sarebbe tecnicamente impossibile, una volta abbinata la chiave di cifratura al messaggio criptato, incorrere in errori di "traduzione", nonché, per altro verso, facendo perno sul principio generale di presunzione di legittimità delle prove acquisite dall'autorità giudiziaria estera. (M.P.)

[Corte di Cassazione, sez. IV penale, 18 aprile 2023 \(ud. 5 aprile 2023\), n. 16347](#)

5. Crittografia, diritto al silenzio e limiti temporali al sequestro di materiale informatico

Non viola il principio di proporzionalità del sequestro informatico la protrazione temporale del vincolo dovuta alla scelta difensiva di non fornire le *password* di accesso al materiale sequestrato. A parere della Suprema Corte, la valutazione circa la "ragionevole durata" del vincolo probatorio deve tenere conto di una serie di fattori, tra cui ruolo primario riveste la difficoltà tecnica di estrazione del dato, anche qualora ciò derivi dalla mancata collaborazione dell'indagato con gli investigatori. In tal caso, dunque, ben potrà operarsi un sequestro *omnibus*, non preceduto da perquisizione informatica "selettiva", che potrà protrarsi finché non sarà superato l'"ostacolo" crittografico. (M.P.)

[Corte di Cassazione, sez. II penale, 27 aprile 2023 \(ud. 23 marzo 2023\), n. 17604.](#)

6. Installazione di apparecchiature atte ad intercettare, impedire o corrompere le comunicazioni informatiche o telematiche e aggravante prevista dagli artt. 617 *quinquies*, co. 2, e 617 *quater*, co. 4, cod. pen.

Ricorre l'aggravante prevista dagli artt. 617 *quinquies*, co. 2, e 617 *quater*, co. 4, cod. pen. nel caso in cui vengano apposti presso gli sportelli "bancomat" i dispositivi denominati *skimmer* atti ad intercettare fraudolentemente comunicazioni di dati. L'attività bancaria di raccolta del risparmio, infatti, costituisce un servizio di pubblica necessità esercitata da soggetti privati, risponde a un interesse pubblico ed è svolta a seguito del rilascio di specifica autorizzazione, sicché qualsiasi attività di intercettazione abusiva di dati a suo danno deve ritenersi esercitata a danno di un esercente un soggetto esercente servizio di pubblica necessità (A.B.)

[Corte di Cassazione, Sez. V penale, 28 aprile 2023 \(ud. 23 gennaio 2023\), n. 17814](#)

7. Stalking online: costituisce reato ai sensi dell'art. 612 *bis* cod. pen. la creazione di falsi profili Facebook riconducibili alla vittima

Costituisce atto persecutorio ai sensi dell'art. 612 *bis* cod. pen. la creazione di falsi profili Facebook e *account* internet falsi riconducibili alla vittima di *stalking* qualora i contenuti postati e l'uso di detti profili si rivelino idonei a realizzare molestie reiterate. Nel sancire il principio ivi descritto, la Corte rivede e perfeziona un orientamento da tempo consolidato in base al quale non può dirsi *stalking* la semplice creazione di un profilo *social* riconducibile alla vittima, aprendo alla possibilità che simile comportamento si traduca in atto persecutorio laddove le modalità di utilizzo dei profili si connotino per particolare offensività (es. veicolando messaggi diffamatori e immagini offensive) (A.B.).

[Corte di Cassazione, Sez. V penale, 13 giugno 2023 \(ud. 17 marzo 2023\), n. 25533](#)

8. Frode informatica: costituisce riciclaggio la messa a disposizione del proprio conto per ostacolare l'identificazione del denaro proveniente dalla commissione del delitto di cui all'art. 640 *ter* cod. pen.

Integra il delitto di riciclaggio la condotta di chi, senza aver concorso nel delitto presupposto, metta a disposizione il proprio conto corrente per ostacolare l'accertamento della delittuosa provenienza delle somme da altri ricavate mediante frode informatica, consentendone il versamento su di esso e provvedendo, di seguito, al loro incasso (A.B.).

[Corte di Cassazione, Sez. II penale, 5 maggio 2023 \(ud. 26 aprile 2023\), n. 19125](#)

9. Truffa online: niente minorata difesa se ci sono contatti diretti fra venditore e acquirente

La Seconda Sezione Penale della Corte di Cassazione ha affermato, in tema di reati contro il patrimonio, che, laddove la vicenda contrattuale successivamente sfociata in truffa abbia avuto origine da una piattaforma informatica, è da escludersi la sussistenza dell'aggravante di cui all'art. 61, n. 5, cod. pen. (cd. minorata difesa) qualora le parti abbiano avuto contatti diretti come messaggi personali e/o conversazioni telefoniche, potendosi desumere da questo genere di interazioni il superamento dello schermo tipicamente esistente tra controparti *online* in favore di un rapporto personale e diretto (A.B.).

[Corte di Cassazione, Sez. II penale, 22 giugno 2023 \(ud. 9 maggio 2023\), n. 27132](#)

10. Accesso abusivo a sistema informatico o telematico da parte di dipendenti o collaboratori

La Corte di Cassazione, nel pronunciarsi in merito a un caso di accesso abusivo a sistema informatico o telematico imputato ad alcuni ex dipendenti di una società all'interno di uno spazio di archiviazione protetto da password (Dropbox), ha evidenziato come, affinché possa ritenersi integrato il delitto di cui all'art. 615 *ter* cod. pen., sia necessario che si individuino nel dettaglio la titolarità dello spazio di archiviazione, la disponibilità e la finalità degli accessi, a prescindere dalla *natura* dei dati ivi contenuti. In questo senso, non sussiste il delitto *de quo* qualora dei dipendenti creino una cartella Dropbox, condividano successivamente la password con la società e, in un secondo momento, modifichino la password rendendo il *cloud* inaccessibile al datore di lavoro e ciò poiché i collaboratori, in quanto proprietari, hanno tutto il diritto di esercitare sullo spazio di archiviazione lo *ius excludendi alios* (A.B.).

[Corte di Cassazione, Sez. V penale, 27 giugno 2023 \(ud. 22 febbraio 2023\), n. 27900](#)

11. L'acquisizione di corrispondenza informatica secondo la Corte costituzionale

Pronunciandosi in merito a un conflitto di attribuzione sollevato dal Senato della Repubblica nei confronti della Procura della Repubblica presso il Tribunale ordinario di Firenze, la Corte costituzionale ha offerto indicazioni di sicuro interesse per la tematica delle indagini informatiche. Premesso che l'acquisizione di messaggi di posta elettronica e *whatsapp* non è qualificabile come intercettazione allorché avvenga in maniera palese e successivamente alla trasmissione e alla ricezione della comunicazione, la Corte ha evidenziato, in primo luogo, che tali comunicazioni rientrano senza dubbio nella nozione di corrispondenza di cui all'art. 15 Cost. In secondo luogo, secondo la Consulta, simili comunicazioni mantengono la natura di corrispondenza anche dopo la ricezione da parte del destinatario, almeno fino a quando la comunicazione non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento "storico". A quest'ultimo proposito, vi è una presunzione, fino a prova contraria, del carattere riservato, allorché i messaggi siano scambiati a una distanza di tempo non particolarmente significativa rispetto al momento in cui dovrebbero essere acquisiti, in particolare quando essi siano ancora custoditi in dispositivi protetti da codici di accesso. A tale conclusione deve pervenirsi, a parere dei giudici, sulla scorta dell'assunto secondo cui degradare la comunicazione a mero documento quando non più *in itinere* sarebbe una soluzione tale da confinare in ambiti angusti la tutela costituzionale prefigurata dall'art. 15 Cost. nei casi, finendo addirittura per azzerarla, di fatto, rispetto alle comunicazioni operate tramite posta elettronica e altri servizi di messaggistica istantanea, in cui all'invio segue immediatamente – o senza uno iato temporale apprezzabile – la ricezione. (M.P.)

[Corte Costituzionale, sent. 27 luglio 2023 \(ud. 22 giugno 2023\), n. 170](#)

12. Definizione di documento informatico ex art. 491-bis c.p.

La Quinta Sezione penale della Suprema Corte ha affermato che, con riferimento al reato di cui all'art. 491-bis cod. pen., deve essere qualificato come documento pubblico con efficacia fidefaciente il registro informatico dell'università sul quale, all'esito di verifica effettuata da operatori individuati attraverso l'impiego di credenziali, vengano riversati i dati risultanti da statini e verbali di esami, al fine di produrre la documentazione attestante la carriera universitaria dello studente. (M.M.)

[Corte di Cassazione, Sez. V penale, 28 luglio 2023 \(ud. 14 luglio 2023\), n. 33285](#)

13. Detenzione di materiale pedopornografico nella cartella delle immagini condivise all'interno di una chat di gruppo su Telegram

La Terza Sezione penale della Corte di Cassazione, in tema di delitti contro la persona, ha affermato che integra la detenzione penalmente rilevante ai sensi dell'art. 600-quater, comma primo, cod. pen. la disponibilità di "file" di contenuto pedopornografico archiviati sul "cloud storage" di una chat di gruppo nello spazio Telegram e accessibili, per il tramite delle proprie credenziali, da parte di ogni componente del gruppo che abbia consapevolmente preso parte ad esso. Sul piano giurico-penale, dunque, non sussiste alcuna differenza tra un'operazione di download dei files e l'accesso incondizionato ad un archivio condiviso tra i partecipanti ad una chat, in quanto in entrambi i casi l'agente conserva la piena e incondizionata possibilità di fruire del materiale archiviato, indipendentemente dalla circostanza che sia stato lui stesso o altri ad aver effettuato l'operazione di salvataggio (A.B.) (M.M.)

[Corte di Cassazione, Sez. III penale, 4 settembre 2023 \(ud. 4 aprile 2023\), n. 36572](#)

CONTRIBUTI DOTTRINALI DI RILIEVO (A.B.) (M.M.)

Archivio della Nuova Procedura Penale

ARIANNA FESTINESE, *Un nuovo criterio di valutazione in tema di data retention: l'esistenza di 'altri elementi di prova'*, fasc. 3/2023, p. 319 ss.

Archivio Penale

MICHELA SIRACUSA, *Il Giano bifronte: autorità e libertà nella data retention. A proposito di una recente pronuncia della Cassazione*, fasc. 2/2023, 1-31.

ALESSANDRA SCALAS, *I confini mobili della digital evidence: una necessaria tassonomia per la tutela delle garanzie*, fasc. 2/2023, 1-34.

FABIO COPPOLA, *Commisurazione della pena e intelligenza artificiale: una ipotesi di lavoro con l'algoritmo Ex-Aequo*, fasc. 2/2023, 1-29.

FEDERICA DE SIMONE, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, fasc. 2/2023, 1-36.

Cassazione Penale

CLAUDIO MARINELLI, *Non sono utilizzabili neppure in sede di giudizio abbreviato i dati di geolocalizzazione relativi ai cellulari, contenuti in tabulati telefonici, acquisiti dalla polizia giudiziaria in assenza del decreto di autorizzazione dell'autorità giudiziaria*, 7-8, 2023, p. 2279 ss.

RENZO ORLANDI, *Usò poliziesco dell'intelligenza artificiale. L'insegnamento del Bundesverfassungsgericht*, 7-8, 2023, p. 2167 ss.

CHIARA ROSSI, *Osservazioni a Cassazione Penale, Sez. III, 19 gennaio 2023, n. 4212. Il concetto di detenzione di materiale pedopornografico*, 7-8, 2023, p. 2319 ss.

Diritto penale e processo

MARTINA NICCOLINI, *Proporzionalità e adeguatezza in tema di sequestro probatorio anche informatico*, 4, 2023, p. 536 ss.

CARLOTTA CONTI, *Condanna per non aver immediatamente cancellato post sulla propria pagina Facebook*, 7, 2023, p. 989 ss.

Diritto di Internet

CHIARA ROSA BLEFARI, *Digital Forensic e svolgimento delle indagini preliminari per reati sessuali in danno dei minori*, 2, 2023, p. 383 ss.

FRANCESCO GIUSEPPE CATULLO, *Il terrorismo degli influencer*, 2, 2023, p. 353 ss.

PAOLA FODERINI, *Diffamazione del parlamentare tramite Facebook: quando opera lo scudo dell'art. 68 Cost?*, 2, 2023, p. 273 ss.

BEATRICE PANATTONI, *La responsabilità penale del blogger per i contenuti diffamatori pubblicati da terzi sul proprio sito*, 2, 2023, p. 361 ss.

BRUNO TASSONE, *Riflessioni su intelligenza artificiale e soggettività giuridica*, 2, 2023, p. 213 ss.

Famiglia e diritto

GABRIELE CIVELLO, *Corruzione di minorenni e utilizzo di videochat*, 8-9/2023, p. 791 ss.

Giurisprudenza italiana

OTTAVIA MURRO, *L'utilizzabilità dei dati di geolocalizzazione: le risposte della giurisprudenza vs il roboante silenzio normativo*, 7, 2023, p. 1676 ss.

La legislazione penale

ROSA MARIA VADALÀ, *L'impianto sanzionatorio "punitivo" della legge sul diritto d'autore: il diritto al ne bis in idem nella permanenza del doppio binario*, 15 aprile 2023.

ANDREA FRANCESCO TRIPODI, *Uomo, societas, machina*, 10 maggio 2023.

Sistema Penale

EUGENIO FUSCO, *Riflessioni e proposte in tema di reati cyber*, 28 aprile 2023.

LEONARDO ROMANÒ, *La responsabilità penale al tempo di ChatGPT: Prospettive de iure condendo in tema di gestione del rischio da intelligenza artificiale generativa*, 17 maggio 2023.

BEATRICE FRAGASSO, *La responsabilità penale del produttore di sistemi di intelligenza artificiale*, 13 giugno 2023.

DONATELLA CURTOTTI – VITTORIO RIZZI – WANDA NOCERINO – ANNA MARIA RUSSITTO – GIUSEPPE GILIBERTI – GABRIELE SCARPA, *Piattaforme criptate e prova penale*, 26 giugno 2023.

MAURIZIO ROMANELLI, *Intelligenza artificiale, influenza sul mercato politico e reati contro la personalità dello stato. La criminalità terroristica*, 29 giugno 2023.

FILIPPO SPIEZIA, *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: Il ruolo di Eurojust*, 14 luglio 2023.

Altri contributi

FEDERICO CONSULICH – MARCO MAUGERI – CARLO MILIA – TOMMASO NICOLA POLI – GIANFRANCO TROVATORE, *AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?*, Quaderni Consob, n. 29, 2023.

GIUSELLA FINOCCHIARO, *Diritto di internet*, IV ed., Bologna 2023, 1-232.