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

Responsabili scientifici: Prof. Lorenzo Picotti e Prof. Luca Lupària - monitoraggio a cura di Alice Baccin, Marco Mattia, Rosa Maria Vadalà, Beatrice Panattoni, Simone Tarantino e Marco Pittiruti - redazione a cura di Alice Baccin, Simone Tarantino e Marco Pittiruti

NOVITÀ SOVRANAZIONALI

1. Cyber Solidarity Act (CSA): raggiunto un accordo sulla proposta di Regolamento UE in materia di cybersicurezza presentata dalla Commissione Europea nell'aprile 2023

In data 20 dicembre 2023, i rappresentanti degli Stati membri dell'Unione, riuniti nel Coreper, hanno raggiunto una posizione comune sulla proposta di Regolamento Europeo avanzata dalla Commissione in materia di cybersicurezza (CSA), tesa a rafforzare i livelli preventivi di monitoraggio e scansione delle minacce informatiche e a velocizzare i protocolli di risposta difensiva in fase di attacco, al contempo fornendo maggiore protezione ai servizi essenziali potenzialmente bersaglio degli attaccanti, come ospedali e servizi pubblici.

Più nello specifico, il meccanismo di solidarietà approntato nel Regolamento verrebbe in rilievo in ipotesi di un eventuale attacco informatico ai danni di uno Stato membro, al fine di intervenire con uno specifico supporto agli apparati bersagliati, dei tavoli di gestione concertata della crisi e delle soluzioni volte al contenimento della minaccia *cyber*.

L'infrastruttura unionale unitaria prevede, secondo il progetto, la creazione di un "cyber-scudo europeo", ossia una fitta rete di centri operativi di sicurezza (*Security Operations Centre - SOC*) nazionali e transfrontalieri in tutta l'Unione, che possano costantemente monitorare i tentativi di attacco e fornire una prima risposta immediata, contrastando dette minacce, anche grazie a tecnologie all'avanguardia quali, ad esempio, l'intelligenza artificiale.

La Proposta prevede, inoltre, il dispiegamento di risorse in ambito preventivo, impegnate nello studio delle vulnerabilità dei sistemi e, conseguentemente, nel loro rinforzo e nello sviluppo di una riserva dell'UE per la cybersicurezza, in grado di riconoscere a partner fiduciari privati il potere di intervenire direttamente in soccorso allo Stato membro in difficoltà. Il tutto anche tramite la cooperazione e la reciproca assistenza tra Stati, favorendo la circolazione di esperti tra i vari Stati.

L'impegno preventivo, infine, fa da contraltare a un meccanismo di riesame degli incidenti di cybersicurezza, che consente una rivalutazione critica dei *breaches*, allo scopo di evitare la loro ripetizione, eventualmente anche con l'intervento degli esperti di ENISA (*European Network and Information Security Agency*).

(S.T. e A.B.)

Il testo del *Cyber Solidarity Act (CSA)* è disponibile a questo [link](#)

2. Europol: pubblicati il cd. Rapporto IOCTA 2023 e lo Spotlight Report sulle frodi online

Europol ha pubblicato, in data 19 dicembre 2023, il rapporto *Internet Organised Crime Assessment (IOCTA) 2023* contenente una retrospettiva dei mutamenti e delle evoluzioni occorse nel mondo del cd. *cybercrime* nei precedenti ventiquattro mesi. In particolare, il *report* contiene un riepilogo dello stato sull'arte della criminalità informatica con alcune evidenze in merito alle tipologie di schemi fraudolenti maggiormente utilizzati, all'incidenza degli attacchi informatici all'interno dell'Unione e alle modalità operative attraverso cui i cybercriminali operano. Collateralmente, sempre Europol ha predisposto alcuni *spotlight report* connessi al tema principale aventi ad oggetto, nello specifico, le frodi online (*Spotlight Report 'Online fraud scheme: a web of deceit'*), gli attacchi *cyber* (*Spotlight Report 'Cyber-attacks: the apex of crime-as-a-service'*) e lo sfruttamento sessuale dei minori in rete (quest'ultimo in fase di pubblicazione).

Lo IOCTA Report 2023 è disponibile a questo [link](#)

Lo *Spotlight Report 'Online fraud scheme: a web of deceit'* è reperibile a questo [link](#) e lo *Spotlight Report 'Cyber-attacks: the apex of crime-as-a-service'* a questo [link](#)

3. Convenzione internazionale sull'Intelligenza Artificiale: in corso le trattative per il primo trattato internazionale in materia

Il Consiglio d'Europa ha reso pubblica nel dicembre 2023 la terza bozza della Convenzione internazionale sull'intelligenza artificiale (CAI) in discussione all'ultima riunione plenaria tenutasi a Bruxelles dal 23 al 26 gennaio 2024. I negoziati, che procedono spediti e vedono coinvolti plurimi *stakeholders* tra cui organizzazioni non governative attive sul tema, esperti e attivisti, dovrebbero definire un testo comune entro il prossimo maggio.

All'interno degli otto capitoli in cui si articola il testo provvisorio, al momento, si snodano i principi fondamentali che si applicheranno all'interno dei 46 Stati membri e di alcuni paesi "osservatori" come Stati Uniti, Giappone, Messico e Israele, contribuendo a tutelare il rispetto dei diritti fondamentali dell'uomo (quali l'equità e la non discriminazione, la trasparenza, la robustezza e la fiducia) e a determinare ogni aspetto della prima regolamentazione comune a carattere transnazionale del settore. (*S.T. e A.B.*)

La bozza della Convenzione è disponibile a questo [link](#)

4. Conferenza interparlamentare sull'intelligenza artificiale: in Europa l'ennesimo confronto tra Stati membri per valutare l'impatto futuro dell'IA in alcuni settori chiave

Si è tenuta a Bruxelles dal 28 al 29 gennaio 2024 la Conferenza interparlamentare sull'intelligenza artificiale organizzata dal Parlamento della Federazione Vallonia - Bruxelles e dal Parlamento della Vallonia nell'ambito della Presidenza belga del Consiglio dell'Unione Europea nel primo semestre 2024.

L'incontro, cui ha preso parte anche l'Italia con alcuni rappresentanti di Camera e Senato, ha previsto dopo i discorsi di apertura quattro sessioni aventi ad oggetto (i) le industrie creative e culturali di fronte all'intelligenza artificiale e il suo impatto sulla vita quotidiana dei cittadini europei, (ii) la didattica nell'era dell'intelligenza artificiale, (iii) il settore sanitario di fronte all'intelligenza artificiale e (iv) le sfide dell'intelligenza artificiale per la *governance* pubblica. Con l'occasione, gli uffici studio di Camera e Senato hanno predisposto un dossier *ad hoc* riepilogando anche i principali ambiti di attività dei due rami del parlamento, nei differenti settori, per implementare e regolamentare l'uso dell'IA, ricordando come l'Italia si sia allineata a Francia e Germania nell'invocare un approccio "umanocentrico" per la regolamentazione dell'AI senza, tuttavia, porre troppi limiti ai sistemi di intelligenza artificiale generativa, come da documento congiunto sottoscritto dai governi di Italia, Francia e Germania in data 30 ottobre 2023 (*A.B.*).

Il dossier della Camera è disponibile a questo [link](#)

La dichiarazione congiunta dei tre governi è reperibile [qui](#)

5. Via libera dell'Unione Europea al primo schema di certificazione sulla sicurezza informatica sui criteri comuni (EUCC)

Il 31 gennaio 2024 la Commissione Europea ha dato il via libera al primo schema di certificazione della sicurezza informatica, redatto da Agenzia Europea per la Sicurezza Informatica (ENISA), volto a rendere più affidabile le infrastrutture tecnologiche all'interno dell'Unione Europea e a riconoscere ai prodotti in linea con i criteri adottati un bollino blu di sicurezza dal punto di vista sia hardware che software. Lo schema - che sostituirà i precedenti schemi di certificazione nazionali precedentemente previsti dall'accordo SOG-IS in conformità alla decisione del Consiglio dell'UE del 31 marzo 1992 (92/242/CEE) in materia di sicurezza dei sistemi informativi e alla successiva raccomandazione del Consiglio del 7 aprile 1995 (1995/144/CE) sui criteri comuni di valutazione della sicurezza delle tecnologie dell'informazione - si inserisce nel quadro delineato dal Cybersecurity Act e dalla Direttiva Nis2 e sarà su base volontaria per i fornitori di tecnologie dell'informazione e servizi di telecomunicazioni. Esso propone due livelli di garanzia basati sul livello di rischio associato all'uso previsto del prodotto, servizio o processo, in termini di probabilità e impatto di un incidente. Obiettivo dello schema è incentivare i fornitori ad aderire allo schema incrementando il livello europeo in materia di cybersicurezza (*A.B.*).

Lo schema approvato dalla Commissione è disponibile al presente [link](#)

6. AI Act: approvato dal Parlamento Europeo il testo finale del Regolamento in materia di intelligenza artificiale

In data 13 marzo 2024 il Parlamento Europeo ha approvato, a larga maggioranza, il testo definitivo del Regolamento Europeo sull'intelligenza artificiale (cd. *AI Act*), la prima normativa al mondo che mira a disciplinare in modo organico il settore degli agenti intelligenti. Il Regolamento – che attende ora l'approvazione finale del Consiglio e la revisione dei giuristi-linguisti – dovrebbe essere pubblicato nella Gazzetta Ufficiale dell'Unione Europea entro la fine dell'attuale legislatura, per entrare in vigore nel 2026, eccezion fatta per i divieti relativi alle pratiche vietate che si applicheranno a partire da sei mesi successivi, ai codici di buone pratiche (nove mesi dopo) e alle norme sui sistemi di IA per finalità generali, compresa la *governance* (dodici mesi dopo) e gli obblighi per i sistemi ad alto rischio (trentasei mesi dopo).

In generale, il Regolamento si fonda sul cd. *risk based approach* ossia sull'individuazione di diversi profili di rischio a seconda delle differenti tipologie di sistemi di A.I., si pone l'obiettivo di realizzare un bilanciamento tra innovazione e protezione, concentrandosi sulle applicazioni con il maggior potenziale di danno per l'essere umano, individuando specifiche misure a seconda dei casi e mantenendo quali capisaldi trasparenza, affidabilità e *human accountability*.

A questo scopo, i criteri di classificazione del rischio - inteso come eventualità di un danno arrecato a un determinato settore o interesse tutelato dalla legislazione - prevedono tre possibili impatti nei diritti fondamentali: basso o minimo, alto ed inaccettabile. In particolare, i sistemi di A.I. che determinano un rischio inaccettabile sulla sicurezza, i mezzi di sussistenza ed i diritti delle persone sono assolutamente vietati, così come parimenti vietata è l'immissione sul mercato, la messa in servizio di sistemi atti ad operare la manipolazione comportamentale cognitiva (mediante tecniche subliminali e comunque ingannevoli) o lo sfruttamento delle vulnerabilità; la categorizzazione o l'identificazione biometrica da remoto ed «in tempo reale», in spazi accessibili al pubblico (con cui l'algoritmo è uno strumento di rilevazione a distanza delle persone fisiche mediante il confronto di dati biometrici detenuti all'interno di dataset mondiali, con l'unica eccezione delle situazioni di minaccia di attacco terroristico, ricerca di vittime di reati gravi o prosecuzione di seri crimini associativi); lo *scraping* non mirato delle immagini facciali da internet o da filmati di telecamere a circuito chiuso per creare database di riconoscimento facciale; il riconoscimento delle emozioni sul luogo di lavoro e negli istituti scolastici (eccetto per motivi medici o di sicurezza, come il monitoraggio dei livelli di stanchezza di un pilota); il *social scoring* (per attribuire l'affidabilità di un gruppo di persone), la categorizzazione biometrica per dedurre dati sensibili (come ad esempio, quelli sanitari, l'orientamento sessuale o religioso). Al contrario, i sistemi ad alto rischio sono sistemi che possono potenzialmente avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali (così come disciplinati nella Carta dei diritti fondamentali dell'UE), ma che superano un attento vaglio di conformità ai requisiti obbligatori dell'affidabilità, determinata in termini di accuratezza, robustezza, trasparenza e tracciabilità. tra i sistemi ad alto rischio rientrano quelli di identificazione biometrica remota (al di fuori delle categorie vietate); quelli utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture critiche digitali, nel traffico stradale delle nuove *smart roads*, nonché quelli relativi alla valutazione dell'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo. Infine, troviamo i sistemi di A.I. a rischio minimo (come videogiochi o filtri spam) saranno esenti da obblighi, ferma restando il dovere di rispetto dei diritti fondamentali.

Al contempo, consapevole dell'impossibilità di fermare il progresso, l'*AI Act* subordina la distribuzione e l'utilizzo dei sistemi IA ad alto rischio a una serie di controlli *ex ante* aventi ad oggetto il rispetto dei requisiti stabiliti dalla legge per ottenere l'accesso al mercato dell'Unione Europea.

Il controllo sulla regolamentazione di questi sistemi sarà attribuito all'Ufficio per l'Intelligenza artificiale, presso la Commissione, il cui personale sarà supportato da un gruppo di ricerca scientifico composto dai più alti esperti indipendenti. Accanto all'Ufficio per l'IA., verranno costituiti un Comitato composto dai rappresentanti degli Stati membri che fungerà da raccordo e coordinamento con l'Unione in qualità di organo consultivo della Commissione, e un forum consultivo formato da *stakeholders* come, ad esempio, grandi aziende europee del settore, PMI, Startup, mondo accademico, studiosi ed esperti della materia.

Per rendere cogente la normativa prevista nel Regolamento, è altresì previsto uno specifico apparato sanzionatorio, con sanzioni pecuniarie quantificate anche sul fatturato annuo globale nell'esercizio finanziario precedente: 35 milioni di euro, o il 7%, per le violazioni relative ad applicazioni di A.I. vietate, 15 milioni di

euro o il 3% per violazioni degli obblighi del regolamento sull'A.I. e 7,5 milioni di euro o l'1,5% per la fornitura di informazioni inesatte, somme non certo irrisorie, anche per le più virtuose e floride società europee. (S.T.)

Il comunicato stampa è disponibile al seguente [link](#), mentre il testo approvato nella versione italiana – in attesa della pubblicazione in Gazzetta Ufficiale – è reperibile [qui](#)

7. Media Freedom Act: approvata la legge europea per la libertà dei media

Contestualmente all'approvazione dell'*AI Act*, il Parlamento Europeo ha approvato, sempre in data 13 marzo 2024, anche il Regolamento europeo che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la Direttiva 2010/13/UE concernente la fornitura di servizi di media audiovisivi. Il nuovo Regolamento sulla libertà dei Media – cd. *Media Freedom Act* – si pone l'obiettivo di proteggere i giornalisti e, più in generale, chi opera nel settore dell'informazione rafforzando la tutela della libertà di stampa e l'indipendenza editoriale, garantendo pubblicità, trasparenza, pluralismo e salvaguardando giornalisti e fornitori di media dalle possibili ingerenze del potere politico. Più nello specifico, il Regolamento chiarisce, infatti, il ruolo degli Stati membri di garanti della pluralità delle fonti di informazione, dell'indipendenza e del corretto funzionamento dei fornitori di media di servizio pubblico che operano all'interno dei propri confini e stabilisce in capo ad essi l'obbligo di garantire in modo efficace l'esercizio della loro attività professionale. Contestualmente, il nuovo *corpus* normativo vieta l'utilizzo di misure coercitive o di *spyware* o altri mezzi di *detection* al fine di ottenere informazioni sulle fonti o di captare le conversazioni riservate ai giornalisti, esclusi i casi in cui ciò non si riveli necessario nel contesto della repressione di reati gravi commessi dai medesimi.

In aggiunta, sempre il *Media Freedom Act* amplia l'ambito di applicazione dei requisiti in materia di trasparenza (es. trasparenza circa la proprietà del mezzo e i finanziamenti ricevuti) e contiene norme precise a tutela del rapporto tra i fornitori di piattaforme *online* e i fornitori di media, impedendo ai primi di esercitare un controllo sui contenuti diffusi e di rimuovere in modo arbitrario i contenuti dei media indipendenti (A.B.)

L'informativa sull'approvazione del *Media Freedom Act* è disponibile [qui](#)

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. ChatGPT: Garante privacy, notificato a OpenAI l'atto di contestazione per le violazioni alla normativa privacy

In data 24 gennaio 2024 Garante per la protezione dei dati personali ha notificato a OpenAI, società che gestisce la piattaforma di intelligenza artificiale ChatGPT, l'atto di contestazione per aver violato la normativa in materia di protezione dei dati personali.

A seguito della lunga ed approfondita istruttoria condotta, seguita dal [provvedimento](#) di limitazione provvisoria del trattamento, emesso lo scorso 30 marzo 2023, l'Autorità stessa ha ritenuto che gli elementi fin qui acquisiti configurino svariate violazioni della normativa europea in materia di trattamento dei dati personali, per cui ora OpenAI (che non ha comunque sede ufficiale nell'Unione europea, ma nonostante ciò ha designato un delegato rappresentante nello Spazio economico europeo) ha 30 giorni di tempo per comunicare le proprie memorie ed attestazioni difensive sulle presunte violazioni contestate. (S.T.)

Articolo consultabile al seguente [link](#)

2. Approvato dal Consiglio dei Ministri il disegno di legge che riforma alcuni reati informatici ed interviene in materia di cybersecurity

Il Consiglio dei Ministri ha licenziato, in data 25 gennaio 2024, il testo definitivo del disegno di legge volto al rafforzamento della cybersicurezza nazionale che prevede, tra le altre, cose, l'innalzamento delle pene per i cybercriminali, l'intensificazione delle misure di sicurezza, un incremento delle funzioni dell'Agenzia per la cybersicurezza nazionale (ACN) e l'adozione, da parte di enti locali e pubblica amministrazione, di sistemi idonei a prevenire e impedire attacchi informatici. Parte integrante del disegno di legge, infatti, è rappresentato

dalla istituzione di obblighi di notifica a carico delle PA in caso di attacco *hacker* (con un correlato sistema di sanzioni in caso di omissione), dall'istituzione di uffici interni incaricati di salvaguardare la sicurezza informatica dei singoli uffici e dalla nomina di referenti per la *cybersecurity*. Del pari, il ddl inasprisce le sanzioni per i reati già previsti come l'accesso abusivo a sistema informatico, ridefinisce il dolo specifico nelle fattispecie a sfondo *cyber* e introduce nuovi aggravanti e reati (es. l'estorsione cibernetica) tesi a garantire una efficace risposta sanzionatoria per talune forme di attacco informatico, come il *ransomware*, pur oggi facilmente riconducibili a una fattispecie di reato esistente (A.B.).

Lo schema del ddl è reperibile al seguente [link](#)

3. Sequestro di dispositivi e sistemi informatici: presentato un emendamento alla proposta di legge che prevede l'introduzione dell'art. 254 ter c.p.p.

Nell'ambito dell'*iter* di approvazione della proposta di legge avente ad oggetto modifiche al codice di procedura penale in materia di sequestro di dispositivi informatici, *smartphone* e memorie digitali - già orientata ad estendere a detta tipologia di misura le garanzie previste dall'ordinamento in tema di intercettazioni - è stato proposto, in data 21 febbraio 2024, un ulteriore emendamento che, nel recepire l'insegnamento della Consulta sul cd. caso Renzi, prevede di introdurre tre diverse fasi del sequestro: (i) apprensione del dispositivo, (ii) duplicazione dei contenuti, selezione ed effettivo blocco dei dati e, da ultimo, (iii) la distruzione del duplicato.

Più nello specifico, in base al testo predisposto dall'emendamento, il GIP dovrebbe disporre il sequestro sulla scorta di due sostanziali requisiti: la necessità di adozione di detta misura per la prosecuzione delle indagini e il rispetto del criterio di proporzione (con possibilità per il PM o per la polizia di procedere in autonomia, salvo convalida nelle successive quarantotto ore). Successivamente, il Pubblico Ministero provvederà alla duplicazione dei contenuti con il coinvolgimento dell'indagato, della persona offesa e dei loro difensori a cui verrà data notizia del giorno e dell'ora in cui verrà conferito l'incarico al consulente tecnico per la duplicazione. A valle della duplicazione, il Pubblico Ministero potrà disporre il sequestro dei dati aventi contenuti non comunicativi solo se strettamente pertinenti al reato per cui si procede, altrimenti, in caso di dati aventi contenuti comunicativi, dovrà chiedere al GIP di attuare la procedura in vigore per le intercettazioni (A.B.).

Il testo dell'emendamento è disponibile [qui](#)

Le slides di sintesi predisposte dal Ministero della Giustizia sono disponibili [qui](#)

NOVITÀ GIURISPRUDENZIALI NAZIONALI ED EUROPEE

1. Sull'inquadramento normativo dell'attività acquisitiva di messaggistica criptata intercorsa sulla piattaforma "SKY ECC"

La Suprema Corte si è soffermata sull'inquadramento normativo dell'attività investigativa di decodifica e di acquisizione di messaggistica criptata custodita su *server* protetti. La necessità di inquadrare a livello normativo siffatta attività scaturiva dal bisogno di verificare l'utilizzabilità nel nostro ordinamento delle *chat* decodificate, raccolte da un'autorità giudiziaria estera ed acquisite nel nostro ordinamento per il tramite di ordine europeo d'indagine. Ciò, in ragione del "principio di equivalenza" enunciato in quella materia, ai sensi del quale l'O.E.I. può essere emesso a condizione che l'autorità dello Stato di emissione verifichi che gli atti di indagine richiesti nell'O.E.I. avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo.

I giudici di legittimità hanno escluso, anzitutto, che la documentazione in discorso possa essere acquisita ai sensi dell'art. 234-*bis* c.p.p. Ciò in quanto, nel caso di specie, l'attività acquisitiva si era concretizzata nella apprensione occulta del contenuto archiviato in un *server*, nonché nel sequestro di relativi dati ivi memorizzati o presenti in altri supporti informatici, nella disponibilità della società che gestiva quella piattaforma di messaggistica. In siffatte ipotesi, infatti, non può dirsi integrato il presupposto di operatività dell'art. 234-*bis* c.p.p. rappresentato dal consenso del legittimo titolare, vale a dire il mittente o il destinatario dei messaggi oppure la medesima società di gestione della piattaforma, dovendo l'autorità giudiziaria straniera essere considerata mero detentore qualificato di quei dati a fini di giustizia.

Per converso, una siffatta attività acquisitiva va inquadrata, con riguardo all'acquisizione di dati "statici", nelle disposizioni dettate in materia di perquisizione e sequestri, in specie nella norma dettata dall'art. 254-*bis* c.p.p., riguardante le ipotesi di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di comunicazioni. Mentre, qualora l'attività acquisitiva riguardi dati "esterni" relativi al traffico telefonico o telematico è necessario far riferimento all'art. 132 d.lgs. 30 giugno 2003, n. 196, così come la disciplina degli artt. 266 ss. c.p.p. è applicabile nell'ipotesi in cui vi sia stata una captazione di comunicazioni telefoniche, ambientali o di flussi telematici in corso, nella fase c.d. "dinamica". (M.P.)

[Cassazione Penale, Sez. VI, ud. 26 ottobre 2023, dep. 2 novembre 2023, n. 44154](#)

2. Prova digitale e dato crittografato: non va garantito alla difesa l'accesso agli algoritmi impiegati per la decodificazione

Due recenti pronunce hanno affrontato il problema delle garanzie difensive in caso di impiego a fini probatori di dati digitali crittografati. Quanto alla sentenza Cass. n. 46390/23, la difesa sosteneva che le *chat* criptate intercorse sulla piattaforma "SKY ECC" fossero inutilizzabili a fini probatori per la mancata ostensione del metodo di decifrazione. Tali dati, invero, erano stati acquisiti dall'autorità giudiziaria francese e consegnati, tramite ordine europeo di indagine, all'autorità giudiziaria italiana con l'apposizione del segreto di Stato. Nel rigettare la doglianza, i giudici di legittimità hanno affermato che il sistema di diritto interno non garantisce alla difesa l'accesso agli algoritmi per la decodifica dei dati criptati, limitandosi, al contrario, a dettare garanzie procedurali a protezione della cd. "catena di custodia" a tutela dell'integrità probatoria, quali la necessità di un atto autorizzativo da parte di attori giudiziari qualificati, l'individuazione dei soggetti che possono acquisire e ritenere i dati e la disciplina della conservazione e consultazione degli stessi.

Analoga tesi è stata sostenuta da Cass. n. 46482/23, secondo cui l'indisponibilità della tecnologia di *hacking* utilizzata per estrarre e mettere in chiaro messaggistica criptata non determina alcuna lesione dei diritti di difesa, atteso che l'ordinamento interno non obbliga alla ostensione degli attrezzi virtuali con cui si sia ottenuta la decodifica di contenuti telematici. Si è precisato, nondimeno, che resta salva la possibilità per l'imputato di allegare anomalie tecniche che facciano fondatamente dubitare della correttezza delle acquisizioni e che depongano per l'inquinamento del risultato. (M.P.)

[Cassazione Penale, Sez. VI, ud. 26 ottobre 2023, dep. 16 novembre 2023, n. 46390](#)

[Cassazione Penale, Sez. VI, ud. 27 settembre 2023, dep. 17 novembre 2023, n. 46482](#)

3. Credit scoring: la Corte di Giustizia esclude che la sola valutazione algoritmica di affidabilità del creditore possa fondare la valutazione della banca circa la stipula o meno del contratto

La Corte di Giustizia si è pronunciata, in data 7 dicembre 2023, in merito alla pratica del cd. *credit scoring* (l'assegnazione automatica di un punteggio predittivo della capacità del creditore di onorare eventuali debiti) stabilendo che confligge con la previsione dell'art. 22 GDPR - che riconosce il diritto dell'interessato a non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato - la scelta della banca di concedere o meno affidamenti sulla base del solo *credit scoring*. La valutazione predittiva circa la solvibilità del creditore, infatti, non può costituire la sola valutazione di un istituto di credito, ma dev'essere valorizzata unitamente ad altri elementi non automatizzati, in linea con quanto previsto dal Regolamento UE che disciplina il trattamento dei dati personali (A.B.).

[Corte di Giustizia dell'Unione Europea, I Sezione, 7 dicembre 2023, C-634/21](#)

4. Accesso abusivo a sistema informatico: il punto della Cassazione sul caso del P.R.A.

L'arresto giurisprudenziale ha riaffermato, in coerenza con l'insegnamento della nota pronuncia "Savarese", come l'accesso (o il mantenimento) nel sistema ancorché con credenziali lecite attribuite all'agente, anche in assenza di divieti espressi, può essere qualificato come "abusivo", quando risulti effettuato per finalità estranee a quelle proprie della funzione esercitata. In altri termini, per giudicare della liceità dell'accesso, ritiene la Corte, occorre aver riguardo non solo alla titolarità astratta del potere esercitato, ma (anche) al suo concreto

esercizio e, quindi, alla finalità perseguita dall'agente, che deve essere confacente alla ratio sottesa al potere di accesso (Cass., Sez. Un. pen., n. 41210 del 18/05/2017).

L'accesso, dunque, può essere ugualmente definito abusivo ove si concretizzi uno sviamento del potere, realizzabile non solo quando l'attività del pubblico ufficiale sia svolta in palese violazione di norme che ne regolano l'esercizio del potere, ma anche quando questa, seppur formalmente lecita, sia esercitata per la realizzazione di un interesse collidente con quello per il quale il potere è attribuito.

Nel caso di specie, è stata confermata la sentenza della Corte di merito che aveva ritenuto responsabile del delitto di cui all'art. 615-ter c.p. il pubblico ufficiale in servizio presso la sezione di Polizia Giudiziaria della Procura della Repubblica di Avellino, il quale si era ripetutamente introdotto all'interno del Pubblico Registro Automobilistico, per effettuare ricerche nell'interesse del suo informatore.

Il Pubblico Registro Automobilistico, nel quale il pubblico ufficiale si è introdotto avvalendosi delle sue credenziali, è un registro, nazionale gestito dall'ACI, nel quale vanno registrate tutte le operazioni che riguardano le vicende circolatorie o gli elementi identificativi riguardanti un veicolo.

I dati riportati all'interno del registro sono pubblici (attenendo il pagamento del corrispettivo dovuto per l'accesso alla sola gestione economica del servizio), ma l'accesso e la relativa gestione, proprio in ragione della funzione pubblicistica svolta dal registro, è rimesso a soggetti qualificati, titolari del riconosciuto potere, come l'agente, che aveva offerto il relativo accesso al suo informatore come corrispettivo per le informazioni in precedenza ricevute, acquisendo e comunicando le notizie richieste evitandogli un pagamento.

Di conseguenza, l'accesso è stato ritenuto abusivo, proprio perché avvenuto per finalità estranee a quelle proprie dell'ufficio, in quanto l'agente aveva esercitato un potere ed un connesso atto di disposizione delle entrate pubbliche a titolo di corrispettivo per le informazioni dovute, *de visu* difforme all'interesse per il quale il potere stesso era stato attribuito (S.T.).

[Cassazione Penale, Sez. V, Sent., \(data ud. 29/11/2023\) 10/01/2024, n. 1161](#)

5. La Corte di Giustizia dichiara illegittima la normativa nazionale che prevede la conservazione *sine die* dei dati biometrici e genetici a fini di giustizia penale

La Corte di Giustizia, a valle del rinvio pregiudiziale promosso dalla Corte suprema amministrativa bulgara, ha affermato che l'art. 4, par. 1, lett. c) ed e) della direttiva (UE) 2016/680 (relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali) deve essere interpretato nel senso che osta a una normativa nazionale che prevede la conservazione, da parte delle autorità di polizia, di dati personali riguardanti persone che hanno subito una condanna penale definitiva per un reato doloso perseguibile d'ufficio a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali - in particolare di dati biometrici e genetici - fino al decesso di detta persona, anche in caso di riabilitazione di quest'ultima, senza che venga posto a carico del titolare del trattamento l'obbligo di esaminare periodicamente se tale conservazione sia ancora necessaria, né riconoscere all'interessato il diritto alla cancellazione di tali dati, dal momento che la loro conservazione non è più necessaria rispetto alle finalità per le quali sono stati trattati, o, eventualmente, il diritto alla limitazione del loro trattamento (A.B.).

[Corte di Giustizia dell'Unione Europea, Grande Sezione, 30 gennaio 2024, C-112/22, NG](#)

6. Utilizzabili come prova documentale le intercettazioni acquisite all'estero mediante ordine europeo d'indagine

Secondo la Suprema Corte sono pienamente utilizzabili nel procedimento penale come prova documentale le conversazioni ottenute mediante chat criptate e i dati comunicativi acquisiti da una autorità giudiziaria estera nell'ambito di attività richiesta con ordine europeo d'indagine e/o consegnati alla giustizia italiana come dati "freddi", poiché raccolti prima dell'arrivo della richiesta di OEI, e ciò in quanto non è compito del giudice italiano valutare la regolarità o meno degli atti di esecuzione dell'attività d'indagine compiuta da un'autorità straniera se è svolta secondo la legislazione del Paese di riferimento (A.B.).

[Cassazione Penale, Sez. I, 18 gennaio 2024, n. 2312](#)

7. Videoriprese tra persone conviventi e art. 615 bis c.p.: lecita solo quando vi sia il consenso dell'altro soggetto espresso in forma chiara e inequivocabile

Con una pronuncia recente la Corte di Cassazione è tornata sul tema delle videoriprese tra persone conviventi, stabilendo come la ripresa di un contenuto effettuata all'insaputa del soggetto coabitante e senza il suo consenso sia condotta idonea ad integrare il reato di interferenze illecite nella vita privata (art. 615 bis c.p.), in linea con quanto già stabilito nel 2003 dalle Sezioni Unite circa il fatto che non sia consentita, neppure al convivente, la registrazione di immagini di vita privata altrui quando non ne sia parte, poiché solo in quest'ultimo caso l'atto di vita privata appartiene anche a chi l'abbia registrato. Non vi è reato, al contrario, quando il regista del video condivide con l'altro soggetto e con il suo consenso l'atto di vita privata oggetto di captazione. Consenso che deve emergere in modo chiaro e inequivocabile, non potendosi ritenere lecita la ripresa qualora la consapevolezza della persona ritratta non sia pienamente dimostrabile (A.B.).

[Cassazione Penale, Sez. V, 2 febbraio 2024, n. 4840](#)

8. Il trasferimento all'autorità giudiziaria italiana, in esecuzione di ordine europeo di indagine, del contenuto di comunicazioni effettuate attraverso criptofonini già acquisite e decrittate dall'autorità giudiziaria estera

La Corte di Cassazione ha diffuso un'[informazione provvisoria](#) circa la soluzione offerta dalle Sezioni Unite ai quesiti sollevati con le ordinanze nn. 47798/23 e 2329/24, entrambe afferenti al tema del trasferimento all'autorità giudiziaria italiana, in esecuzione di ordine europeo di indagine, del contenuto di comunicazioni effettuate attraverso criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera.

Le Sezioni Unite hanno ritenuto che il trasferimento dei dati di cui sopra rientra in un'acquisizione di atti di altro procedimento penale. Siffatta circolazione probatoria, a seconda della natura di tali atti, trova alternativamente il suo fondamento negli artt. 78 disp. att. c.p.p., 238, 270 c.p.p. e, in quanto tale, rispetta l'art. 6 della Direttiva 2014/41/UE. Tale trasferimento non deve oggetto di verifica giurisdizionale preventiva della sua legittimità nello Stato di emissione dell'ordine europeo di indagine, rientrando l'acquisizione di atti di altro procedimento penale tra i poteri del pubblico ministero. L'utilizzabilità dei dati in discorso è, per converso, soggetta a vaglio giurisdizionale nello Stato di emissione dell'ordine europeo di indagine, dovendosi verificare il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo. (M.P.)

[Cassazione Penale, Sez. III, ord. 3 novembre 2023, n. 47798](#)

[Cassazione Penale, Sez. VI, ord. 15 gennaio 2024, n. 2329](#)

[Memoria della Procura Generale per l'udienza delle Sezioni Unite Penali del 29 febbraio 2024](#)

NOVITÀ RILEVANTI A LIVELLO NAZIONALE

1. Resoconto attività 2023 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica

Il 31 dicembre 2023 la Polizia postale ha redatto il proprio resoconto sugli interventi effettuati nell'ambito della lotta al *cybercrime*, evidenziando un aumento dei casi di reati commessi mediante l'uso del mezzo informatico e il sempre maggiore coinvolgimento, in qualità di vittime, di minori (bambini o preadolescenti tra i 10 ed i 13 anni), i quali rischiano di finire nella rete di pedofili, adescatori cibernetici (206 casi), cyberbulli (284 casi) o di cadere vittime di ricatti e *sextortion* (136 casi) all'interno dei *social media*.

La Polizia, infatti, ha condotto molteplici operazioni per combattere questi fenomeni (solo per menzionarne alcune: Operazioni “*Fast and done*”; “*Ciaoamigos*”; “*Lucignolo*”), grazie alle quali molteplici indagati sono stati sottoposti a perquisizione domiciliare e poi all'esecuzione di misure cautelari restrittive della libertà personale per reati come la detenzione di materiale pedopornografico reperito *online*, la violenza sessuale documentata a danno di minori, lo sfruttamento della prostituzione minorile e la pornografia minorile.

Del pari, accanto alla lotta alla pedopornografia, l'attività della Polizia Postale si è concentrata sul contrasto alle attività predatorie online (oltre 3.500 le persone deferite all'A.G.), in particolare nel settore dell'e-

commerce. Nel 2023, infatti, sono incrementati in numero significativo i casi di trading *online* ingannevole (3.360 i casi trattati, 188 le persone denunciate per un totale di 109.536.088 euro di profitti illeciti), con l'aumento del numero di portali che propongono programmi speculativi, apparentemente redditizi, utilizzando tecniche molto sofisticate per contattare le vittime.

Le evidenze acquisite nella più recente azione di contrasto ai fenomeni criminali di carattere finanziario hanno permesso di registrare una persistente diffusione di condotte predatorie realizzate attraverso campagne di *phishing* (anche nelle varianti del c.d. "*vishing*" e del c.d. "*smishing*": illecita raccolta di codici "*one-time*", token virtuali e *password*, realizzato mediante il ricorso a chiamate o messaggi la cui provenienza sembra essere della banca o di un ente fiduciario, ma che invece sono fraudolenti) consumate non solo nei confronti di persone fisiche, ma anche e soprattutto giuridiche, perpetrate per il tramite di e-mail che, dietro apparenti comunicazioni di Ministeri, organizzazioni pubbliche, istituti di credito ed altri enti, consentono in realtà di acquisire i dati personali e sensibili, le *password* di accesso a domini riservati, utili per perpetrare reati contro il patrimonio.

A ciò si aggiungono la lotta e il contrasto ai reati che hanno ad oggetto la tutela delle vittime di violenza domestica e di genere, reati ricompresi nell'alveo del c.d. *Codice Rosso* (L. 19 luglio 2019, n. 69) per cui 31 sono stati i casi di intervento da parte della Polizia Postale.

Infine, consistente è stato l'impegno della Polizia Postale sul fronte della lotta al cyberterrorismo e, più in generale, all'*hate speech* e alla diffusione di messaggi propagandistici di varia natura e origine su piattaforme di comunicazione *online*, *social network* e app di messaggistica istantanea

Di fronte a tutti questi rischi cibernetici, dunque, è necessario mantenere un alto livello di attenzione e di controllo soprattutto sull'operato e le comunicazioni che riguardano minori, i quali rimangono i target più ricercati dai predatori online. (S.T.).

Il report della Polizia Postale è reperibile [qui](#)

2. Cybercrime, oltre 17mila frodi creditizie in Italia nel 2023 secondo quanto riferito dall'Osservatorio CRIF sui furti d'identità e le frodi creditizie

L'indagine condotta dall'Osservatorio sui furti d'identità e le frodi creditizie di CRIF ha evidenziato come le frodi mediante furto di identità continuano ad avere un rilevante impatto nella geografia criminale italiana, tanto che nel primo semestre del 2023 si sono registrati oltre 17.000 casi con profitti per oltre 83 milioni di euro e un aumento complessivo dei casi del 14,2%. Se da un lato, infatti, sono gli uomini ad essere il bersaglio preferito degli attacchi informatici - con una percentuale del 66,1% contro il 33,9% delle donne - dall'altro, contrariamente a quanto si potrebbe pensare, la fascia d'età maggiormente colpita è quella tra i 18 ed i 30 anni, con una percentuale del 23,8%, più avvezzi ad operare e ad effettuare pagamenti *online*.

I mezzi più frequenti tramite cui queste frodi vengono effettuate sono, in ordine, i prestiti finalizzati (37,9%), le carte di credito (17,5%, in aumento) e i prestiti personali che, nel primo semestre del 2023, hanno registrato un notevole incremento dei casi (+61,2%), con una quota pari al 18,3% del totale dei casi stimati.

La lotta alla criminalità informatica, per essere efficace, necessita di una risposta rapida che, secondo l'Osservatorio, si ha nel 45,5% dei casi (entro 6 mesi dall'accaduto), pur essendo ancora alta la percentuale di scoperta delle frodi dopo cinque anni - che si attesta al 21,8% - per le quali diventa estremamente difficile anche l'intervento dell'Autorità giudiziaria. (S.T.)

Articolo fruibile al seguente [link](#)

VOLUMI E CONTRIBUTI DOTTRINALI DI RILIEVO (A.B.) (S.T.) (M.P.)

Altalex

DI SANTO, *L'intelligenza artificiale al servizio della giustizia penale?*, 23/01/2024

Archivio penale

DELLA TORRE-MALACARNE, *L'utilizzo dei file di log per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni*, fasc. 3/2023 web, 22 dicembre 2023

DINACCI, *I modi acquisitivi della messaggistica chat o e-mail: verso letture rispettose dei principi*, fasc. 1/2024 web, 18 gennaio 2024

GALLO, *Un altro tassello giurisprudenziale in tema di Ordine Europeo d'Indagine penale (OEI) per l'acquisizione della digital evidence dal server estero*, fasc. 3/2023 web, 28 novembre 2023

VELE, *Aspetti critici del documento probatorio "screenshot" e acquisito mediante il captatore informatico*, fasc. 1/2024 web, 8 marzo 2024

Banca Borsa Titoli di Credito

TOLA, *Valute virtuali e frode alla legge*, fasc. 6/2023, p. 794 ss.

Cassazione Penale

CASCONE, *La normativa spagnola in materia di misure di investigazione tecnologica nell'indagine penale: alcuni possibili spunti per il legislatore italiano per un approccio sistematico alla materia*, fasc. 9/2023, p. 3006 ss.

LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali criptate nella fucina dell'ordine europeo d'indagine*, fasc. 1/2024, p. 180 ss.

NOCERINO, *L'acquisizione della messaggistica su sistemi criptati: intercettazioni o prova documentale?*, fasc. 9/2023, p. 2786 ss.

SPANGHER, *Criptofonini: sono "in gioco" diritti fondamentali*, fasc. 1/2024, p. 173 ss.

TRIPICCIÓN, *Il regime di utilizzabilità della prova digitale formata all'estero ed acquisita tramite ordine europeo di indagine*, fasc. 2/2024, p. 692 ss.

Diritto dell'Informazione e dell'Informatica

CURTOTTI, *La sentenza costituzionale n. 170 del 2023 e le comunicazioni "apparenti": quando un eccesso di garanzie non sempre è un moltiplicatore di garanzie*, fasc. 5/2023, p. 708 ss.

CERQUA-LUPÁRIA, *La versione della Consulta sulla corrispondenza elettronica. Un bouleversement in materia di prova digitale?*, fasc. 5/2023, p. 718 ss.

ORLANDI, *"Corrispondenza" dei parlamentari e limiti all'accertamento penale. Appunti critici sulla sentenza nr. 170/2023 della Corte costituzionale*, fasc. 5/2023, p. 730 ss.

SAMMARCO, *Perplessità sull'immunità parlamentare in tema di corrispondenza*, fasc. 5/2023, p. 738 ss.

SPANGHER, *Dopo i parlamentari servono garanzie per gli imputati*, fasc. 5/2023, p. 742 ss.

ZENO-ZENCOVICH, *La “corrispondenza digitale”*: notazioni comparate da oltre-Atlantico, fasc. 5/2023, p. 744 ss.

Diritto di Internet

BARRESI, *Gli incerti contorni del trattamento illecito di dati personali: tra passi indietro e pericolosi consolidamenti*, fasc. 4/2023, p. 761 ss.

CERQUA, *“La piazza virtuale” ovvero l’impiego della metafora per l’addomesticamento dell’ignoto. Il caso di vilipendio della bandiera della Unione Europea*, fasc. 4/2023, p. 777 ss.

MATTIA, *Sul concetto di “detenzione dematerializzata” di materiale pedopornografico rispetto al contesto delle chat di gruppo*, fasc. 4/2023, p. 747 ss.

MONZILLO, *La restituzione dello smartphone e della copia forense: un rimedio “mite”*, fasc. 1/2024, p. 112 ss.

PICOTTI, *Per un inquadramento dei profili penali della sanità digitale, Stati Generali del diritto di internet e dell’intelligenza artificiale*, supplemento al fasc. 1/2024.

Diritto penale e processo

CECCHI, *Mancanza di tutela in un caso di intercettazioni casualmente criptate*, fasc. 2/2024, p. 279.

CISTERNA, *Il contrasto al terrorismo online e la tutela delle infrastrutture informatiche*, fasc. 11/2023, p. 1431 ss.

FONTANI, *La svolta della consulta: la “corrispondenza telematica” è pur sempre corrispondenza*, fasc. 10/2023, p. 1312 ss.

Giurisprudenza italiana

ERRICO, *Sequestro preventivo di valute virtuali, tra incertezze e prospettive*, fasc. 2/2024, p. 435 ss.

GIOIA, *Il valore probatorio dello screenshot tra processo civile e processo penale*, fasc. 12/2023, p. 2623 ss.

MORCELLA, *Da mihi factum, dabo tibi ius: un principio irrinunciabile, pure nell’era dei criptofonini*, fasc. 10/2023, p. 2191 ss.

MORCELLA, *Ed ora, come si può apprendere la corrispondenza archiviata?*, fasc. 1/2024, p. 195 ss.

La legislazione penale

FEDERICI, *Il concetto di materiality (“comune” e “tecnico”) negli abusi di mercato e nel falso in bilancio: un’indagine comparata*, 2/2024.

Processo penale e giustizia

MIRAGLIA, *Il “Trojan (non) di Stato”*: una disciplina da completare, fasc. 5/2023, p. 1227 ss.

PASCAZIO, *Nessun dietrofront sull'utilizzabilità della messaggistica decriptata da autorità giudiziaria straniera*, fasc. 6/2023, p. 1328 ss.

VIRGA, *Lost in translation: le intercettazioni per instradamento di chat crittografate*, fasc. 5/2023, p. 1142 ss.

Rivista Italiana di Diritto e Procedura Penale

BEGUINOT, *I reati contro la sfera sessuale della persona al tempo di internet, tra criticità tradizionali ed esigenze di prevenzione*, fasc. 3/2023, p. 1001 ss.

PAGELLA, *Responsabilità penale di un aspirante deputato per i commenti islamofobi pubblicati da terzi sulla sua pagina Facebook: la corte EDU sui limiti di manifestazione del pensiero*, fasc. 3/2023, p. 1243 ss.

Sistema Penale

DANIELE, [Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite](#), 11 dicembre 2023

DE FLAMMINEIS, [Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale](#), 8 marzo 2024

FLORIO, [Il dibattito sulla responsabilità penale diretta delle IA: "molto rumore per nulla"?](#), fasc. 2/2024, p. 5 ss.

NICOLICCHIA, [A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla querelle giurisprudenziale sull'acquisizione di messaggistica criptata dall'estero](#), fasc. 2/2024, p. 189 ss.

ORLANDO, [Mutua ammissibilità della prova tra gli Stati membri dell'Unione europea ed e-evidence: riflessioni a margine della proposta di direttiva dello European Law Institute](#), fasc. 11/2023, p. 19 ss.

RAGAZZI-SPIEZIA, [Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del count-down italiano](#), fasc. 2/2024, p. 203 ss.

Volumi:

Collana del Dipartimento di Scienze Giuridiche dell'Università di Verona

PICOTTI (a cura di), *Automazione, Diritto e Responsabilità*, Atti del Convegno di Studi del 21-22 ottobre 2022 conclusivo della ricerca condotta dal team "Automazione, Diritto e Responsabilità" (AUDIRR) nell'ambito del Progetto d'eccellenza del Dipartimento di Scienze Giuridiche dell'Università di Verona, E.S.I., 2023, pp. I-X, 1-392.

Revue Internationale de Droit Pénal (RIDP)

LELIEUR, *Artificial intelligence and Administration of criminal Justice*, (*International Colloquium*, Buenos Aires, Argentina, 28-31 March 2023), Vol. 94 issue 2, 2023, pp. 1-392.