News giugno 2021

Responsabile scientifico: prof. Lorenzo Picotti - monitoraggio a cura di Chiara Crescioli, Beatrice Panattoni e Rosa Maria Vadalà

NOVITÀ SOVRANAZIONALI

1. Diritto d'autore e responsabilità dei gestori dei servizi di *hosting*

L'articolo 3 paragrafo 1 della direttiva 2001/29/CE del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (direttiva sul diritto d'autore), deve essere interpretato nel senso che il gestore di una piattaforma di condivisione di video o di una piattaforma di *hosting* e di condivisione di file, sulla quale utenti possono mettere illecitamente a disposizione del pubblico contenuti protetti, non effettua una «comunicazione al pubblico» di detti contenuti, ai sensi di tale disposizione, salvo che esso contribuisca, al di là della semplice messa a disposizione della piattaforma, a dare al pubblico accesso a siffatti contenuti in violazione del diritto d'autore. Ciò si verifica, in particolare, qualora tale gestore sia concretamente al corrente della messa a disposizione illecita di un contenuto protetto sulla sua piattaforma e si astenga dal rimuoverlo o dal bloccare immediatamente l'accesso ad esso, o nel caso in cui detto gestore, anche se sa o dovrebbe sapere che, in generale, contenuti protetti sono illecitamente messi a disposizione del pubblico tramite la sua piattaforma da utenti di quest'ultima, si astenga dal mettere in atto le opportune misure tecniche che ci si può attendere da un operatore normalmente diligente nella sua situazione per contrastare in modo credibile ed efficace violazioni del diritto d'autore su tale piattaforma, o ancora nel caso in cui esso partecipi alla selezione di contenuti protetti comunicati illecitamente al pubblico, fornisca sulla propria piattaforma strumenti specificamente destinati alla condivisione illecita di siffatti contenuti o promuova scientemente condivisioni del genere, il che può essere attestato dalla circostanza che il gestore abbia adottato un modello economico che incoraggia gli utenti della sua piattaforma a procedere illecitamente alla comunicazione al pubblico di contenuti protetti sulla medesima.
Per quanto riguarda invece il regime di responsabilità delineato dall'articolo 14 paragrafo 1 della direttiva 2000/31/CE (direttiva sul commercio elettronico), rientra nel suo ambito di applicazione l'attività del gestore di una piattaforma di condivisione di video o di una piattaforma di *hosting* e di condivisione di file, purché detto gestore non svolga un ruolo attivo idoneo a conferirgli una conoscenza o un controllo dei contenuti caricati sulla sua piattaforma. È dunque escluso dal beneficio dell'esonero dalla responsabilità previsto da tale disposizione il gestore che sia al corrente degli atti illeciti concreti dei suoi utenti relativi a contenuti protetti che siano stati caricati sulla sua piattaforma.

Corte di Giustizia dell'Unione Europea, Grande Sezione, 22 giugno 2021, cause riunite C-682/18 e C-683/18

2. Violazione della proprietà intellettuale in reti *peer to peer*

Sulla base dell'articolo 3, paragrafi 1 e 2, della direttiva 2001/29/CE del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, costituisce messa a disposizione del pubblico il caricamento, a partire dall'apparecchiatura terminale di un utente di una rete *peer-to-peer* verso apparecchiature terminali di altri utenti di tale rete, dei segmenti di un file multimediale contenente un'opera protetta, benché tali segmenti siano utilizzabili autonomamente soltanto a partire da una determinata percentuale di scaricamento e l'utente finale, previamente informato, abbia dato il suo consenso.
L'articolo 6, paragrafo 1, primo comma, lettera f), del Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in combinato disposto con l'articolo 15, paragrafo 1, della direttiva 2002/58/CE del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, come modificata dalla direttiva 2009/136/CE del 25 novembre 2009, deve essere interpretato nel senso che esso non osta, in linea di principio, né alla registrazione sistematica, da parte del titolare dei diritti di proprietà intellettuale, nonché di un terzo per suo conto, degli indirizzi IP di utenti di reti *peer-to-peer* utilizzate per violazioni di questi diritti, né alla comunicazione loro dei nomi e degli indirizzi

postali di tali utenti al fine di consentirgli di proporre un ricorso per risarcimento danni dinanzi a un giudice civile, a condizione, però, che queste iniziative abbiano fondamento normativo nazionale e siano proporzionate e non abusive.

In senso conforme: Corte di Giustizia dell'Unione Europea, Grande Sezione, 7 agosto 2018, C-161/17; Corte di Giustizia dell'Unione Europea, Grande Sezione, 9 marzo 2021, C- 392/19 (consultabile nella raccolta di novità del mese di marzo 2021).

Per approfondire: FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale*, Padova, 2010; ID., *La tutela penale dei diritti d'autore e connessi*, in CADOPPI A., CANESTRARI S., MANNA A. e PAPA A. (a cura di), *Cybercrime*, Torino, 2019, p. 1045 ss.

Corte di Giustizia dell'Unione Europea, Sezione V, 17 giugno 2021, causa C-597/19

3. L'anonimizzazione e la libertà di espressione on line

L'anonimizzazione, nell'archivio digitale di un giornale, di un articolo indicante il nominativo completo del responsabile di un omicidio stradale, verificatosi 20 anni prima, condannato e già riabilitato, costituisce misura idonea a garantire il giusto bilanciamento tra il diritto al rispetto della vita privata del soggetto responsabile -, il quale include altresì il diritto ad essere dimenticato - e la libertà di espressione. Pur non sussistendo in conseguenza del decorrere del tempo dal fatto di cronaca riportato un obbligo di verifica dei relativi contenuti presenti negli archivi online dei giornali, l'anonimizzazione costituisce rimedio doveroso in caso di espressa richiesta dell'interessato, al fine di evitare che la permanenza della notizia online si trasformi in un "*virtual criminal record*" che continui ininterrottamente a danneggiarne la reputazione.

Per approfondire: PAPA A., *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*, Torino, 2009; DI CIOMMO F., *Quello che il diritto non dice. Internet e oblio*, in *Danno resp.*, 2014, n. 12, p. 1101 ss.; R. FLOR, *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?,* in *Dir. inf.*, 2014, n. 4-5, p. 775 ss.; MAZZANTI E., *Eternal Sunshine of the Spotless Crime. Informazione e oblio nell'epoca dei processi su internet*, in *Diritto Penale Contemporaneo - Rivista trimestrale*, 2019, n. 2, p. 212 ss.; PANATTONI B., *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel Cyberspace*, in *Sistema Penale*, 2020, n. 5, p. 303 ss.; GIMIGLIANO S., *Quando il tempo sposta l'ago della bilancia. Spunti sul diritto all'oblio dalla giurisprudenza penale di legittimità,* in *Giurisprudenza penale web*, 2020, *n.* 3.

Corte europea diritti dell'uomo, 22 giugno 2021, app. n. 57292/16, Hurbain v. Belgium

4. Analisi della consultazione *multi-stakeholder* tenuta dalla Comitato *ad hoc* sull'Intelligenza Artificiale del Consiglio d'Europa

Il comitato *ah hoc* del Consiglio d'Europa sull'Intelligenza Artificiale (*Ad hoc Committee on Artificial Intelligence*, CAHAI), dopo aver pubblicato nel 2020 uno studio che esaminava le ragioni per cui risulta necessario elaborare un adeguato quadro normativo per la protezione dei diritti umani, la democrazia e il principio di legalità di fronte alle sfide poste dai sistemi di AI, ha avviato una consultazione da marzo a maggio 2021, rivolta a diversi attori pubblici e privati del settore, i cui risultati vengono riepilogati e commentati in questo report.
Le questioni analizzate riguardano la definizione di "*AI system*", le opportunità e i rischi legati a tali sistemi, le potenziali lacune nelle fonti normative vigenti ritenute applicabili al settore, gli elementi e i principi che dovrebbero essere ricompresi da un quadro normativo relativo ai sistemi di AI, e, infine, le scelte e le proposte di politiche e misure legislative da assumere.
Nell'analisi dei rischi legati alla protezione dei diritti umani, della democrazia e del principio di legalità, le risposte raccolte segnalano un maggior grado di rischio in relazione alle aree della *law enforcement,* della

giustizia, dei *social networks*, della sicurezza nazionale e della lotta al terrorismo. Mentre tra le tipologie di applicazioni di AI percepite e valutate quali maggiormente rischiose figurano i sistemi utilizzati dalle autorità pubbliche per lo *scoring* dei cittadini e il riconoscimento facciale utilizzato a supporto delle forze dell'ordine. Tra l'analisi degli strumenti normativi da utilizzare per colmare le lacune eventualmente riscontrate, si registra un ampio consenso nel ritenere i meccanismi di *self-regulation* meno efficienti rispetto a fonti di *hard law* (41, 5%), nonché generalmente insufficienti ~~e~~ per mitigare e prevenire i rischi di violazioni di diritti umani (53, 9%).

Ad Hoc Committee on Artificial Intelligence (CAHAI) of the Council of Europe, Analysis of the Multi-Stakeholder Consultation

5. Raccomandazione della Commissione europea sull'istituzione di un'unità congiunta per il *cyberspace*

La Commissione europea, evidenziando come la cybersicurezza sia divenuta essenziale per un'efficace trasformazione digitale dell'economia e della società, vista la sempre maggior dipendenza dell'Europa da reti e sistemi informatici, fortemente accresciuta e divenuta evidente con la pandemia Covid-19, ha evidenziato l'opportunità di creare una piattaforma unica e comune a livello europeo volta a coordinare gli sforzi dell'UE per prevenire, rilevare, scoraggiare, contrastare e attenuare le crisi e gli incidenti informatici su vasta scala (ossia «eventi con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi», *ex* art. 4 punto 7 direttiva UE/2016/1148, aventi un impatto significativo in almeno due Stati membri). A tal fine la Commissione afferma, articolandone le fasi e tempistiche d'istituzione, la necessità di creare un'unità congiunta per il cyberspazio, che consenta di garantire una risposta coordinata agli incidenti attraverso, tra le altre, l'istituzione di gruppi di reazione rapida dell'UE per la cybersicurezza e la realizzazione coordinata di una piattaforma virtuale e fisica quale infrastruttura di supporto per la cooperazione tecnica e operativa tra i partecipanti.

Raccomandazione (UE) 2021/1086 della Commissione del 23 giugno 2021 sull'istituzione di un'unità congiunta per il ciberspazio

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Le nuove disposizioni in materia di *cybersecurity*

Nella Gazzetta ufficiale n. 140 del 14 giugno 2021 è stato pubblicato il d.l. 14 giugno 2021, n. 82, rubricato "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale". Con tale disposizione legislativa viene istituita la nuova Agenzia per la cybersicurezza nazionale, allo scopo di coordinare i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuovere la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché il conseguimento dell'autonomia, nazionale ed europea, con riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. In particolare, tra i diversi compiti attribuiti alla nuova agenzia dall'art. 7 del d.l. vi sono quello di predisporre la strategia nazionale di cybersicurezza, di sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, cura e promuove la definizione, di mantenere un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, anche esprimendo pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza e di coordinare la cooperazione internazionale nella materia della cybersicurezza. Inoltre, all'art. 10 viene prevista l'adozione di una nuova procedura per la gestione delle crisi che coinvolgono aspetti di cybersicurezza.

Decreto-Legge 14 giugno 2021, n. 82, disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale

In argomento, con riferimento al d.l. 105/2019, conv. in l. 133/2019, si vedano PICOTTI L., *Cybersecurity: quid novi?*, in *Diritto di Internet*, 2020, n. 1, p. 11 ss.; ID. e VADALA' R.M., *Sicurezza cibernetica: una*

nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti, in www.sistemapenale.it, 5 marzo 2019; MELE S., *Il perimetro di sicurezza nazionale cibernetica*, *ivi*, p. 15 ss..

2. La Relazione della Consob sull'anno 2020

Nel presentare in data 14 giugno 2021 la Relaziona annuale sull'anno 2020 il Presidente della Consob ha messo in luce l'urgenza d'intervenire sulla regolamentazione delle innovazioni finanziarie e in particolar modo sul variegato ecosistema delle *cryptocurrency*: "*Senza presidi adeguati (norme ed enti), ne consegue un peggioramento della trasparenza del mercato, fondamento della legalità e delle scelte razionali degli operatori. Tra gli effetti negativi ben conosciuti vi è la schermatura che queste tecniche consentono ad attività criminali, come l'evasione fiscale, il riciclaggio di denaro sporco, il finanziamento del terrorismo e il sequestro di persone*".
Le preoccupazioni segnalate derivano dal registrato aumento, attestato dalla Relazione, dei casi di prestazione abusiva di servizi d'investimento e offerta abusiva di prodotti finanziari in prevalenza sul web. Nonostante il livello di attività dei risparmiatori in cripto-valute, *trading on line*, *robo advice* e *crowdfunding* risulti ancora contenuto, è rapidamente e significativamente cresciuto sia per effetto della pandemia, sia per l'accelerazione delle iniziative FinTech.
Nello specifico, nel corso del 2020 si è assistito ad un incremento delle offerte abusive aventi ad oggetto *digital token* emessi nell'ambito di autentiche o presunte operazioni di *Initial Coin Offering* (ICO), nonché delle proposte di investimenti finanziari 'atipici' relativi a presunte cripto-valute con apparenti rendimenti del tutto fuori mercato. È indicato come schema tipico di truffe in *trading on line* il seguente meccanismo: il risparmiatore, mosso dalla prospettiva di facili guadagni a fronte di investimenti iniziali di modica entità, viene invitato a fornire i propri dati personali e a versare somme di denaro d'importo via via crescente per aprire i conti per il *trading* di titoli presso la piattaforma online indicata dall'operatore abusivo. Non di rado gli è offerta, come ulteriore incentivo ad investire, la possibilità di avvalersi anche per lo svolgimento dell'attività di *trading* di *software* che realizzano operazioni di investimento secondo modalità automatiche. Ma al momento di incassare i presunti guadagni maturati, l'investitore si vede negata la possibilità di prelevare in tutto o in parte le somme che risultano presenti sul conto, con i pretesti più disparati. Ulteriori fattispecie ricorrenti, sulle quali la Consob ha pubblicato avvisi ai risparmiatori, riguardano l'utilizzo illegittimo da parte di operatori finanziari abusivi del nome e dell'immagine di personaggi noti ed offerte fittizie via web d'investimenti in qualche modo collegati alla pandemia, come quelli in *Corona-coin*, valute virtuali correlate alla diffusione del contagio. Dai risultati raccolti emerge, inoltre, che gli operatori abusivi sono spesso società fittizie o extraeuropee, in apparenza localizzate in paesi europei, ma in realtà irreperibili, che dichiarano spesso falsamente di essere autorizzate a operare. Per questi casi ed in generale per le ipotesi di abusivismo per violazione delle disposizioni in materia di emittenti (offerta al pubblico di prodotti finanziari e pubblicità relativa all'offerta al pubblico di prodotti finanziari in assenza di pubblicazione del prospetto) e di intermediari (prestazione abusiva di servizi di investimento) la Consob ha avviato 348 istruttorie nel corso del 2020, adottando 185 ordini di oscuramento riferibili a 237 siti internet ed inoltrando in 208 casi segnalazioni all'Autorità Giudiziaria per la possibile ricorrenza di profili di abusivismo penalmente rilevanti ai sensi dell'art. 166 del Tuf .
La Consob intende, inoltre, affrontare le sfide poste del web e dal ricorso alle nuove tecnologie proseguendo la transizione tecnologica in atto dell'Istituto. È, in particolare, previsto il potenziamento della vigilanza *data driven* e l'avvio di sperimentazioni per l'impiego dell'intelligenza artificiale, con promozione di quelle iniziative che garantiscano elevati livelli di *cybersecurity*.

Discorso del Presidente della Consob al mercato e Relazione annuale

3. Quaderno n. 16 dell'antiriciclaggio dell'UIF: Casistiche di riciclaggio e di finanziamento del terrorismo

In conformità alle caratteristiche dello strumento, che vuole essere di ausilio ai destinatari degli obblighi antiriciclaggio nella rilevazione di fenomeni di riciclaggio e finanziamento del terrorismo, sono descritte alcune ipotesi rilevanti individuate dall'Unità d'Intelligenza Finanziaria, UIF, nella sua esperienza operativa, attraverso le segnalazioni di operazioni sospette, gli accertamenti ispettivi, gli scambi informativi con le *Financial Intelligence Unit* estere (FIU).

Per ogni fattispecie è previsto un breve *abstract,* che ne riassume, nel rispetto dei presidi di riservatezza, i tratti fondamentali e l'esito degli approfondimenti effettuati dall'UIF, nonché gli indicatori di anomalia ritenuti esemplificativi.
La selezione dei casi riportati conferma la crescente complessità degli schemi operativi delle attività di riciclaggio e finanziamento del terrorismo: dall'utilizzo di sofisticate triangolazioni al ricorso a strumenti di pagamento innovativi, in connessione con fenomeni criminali come criminalità organizzata, corruzione ed evasione fiscale.
Questo intreccio è messo in evidenzia nel caso trattato di riciclaggio dei proventi derivanti dal traffico di sostanze stupefacenti: sulla base di informazioni di fonte estera, l'UIF è risalita a proventi illeciti in valute virtuali derivanti dal traffico di sostanze stupefacenti gestito, tramite diverse piattaforme sul c.d. *dark web*, da un'organizzazione operante tra l'Italia e il Nord America. Le somme in valute virtuali venivano convertiti in valute aventi corso legale e accreditati su conti correnti italiani per essere ritrasferiti, poi, in Nord America mediante rimesse ed acquisti di auto di lusso.

Quaderno dell'antiriciclaggio n. 16 di giugno 2021

4. Rapporto UIF per il 2020

In data 24 giugno 2021 è stato presentato il Rapporto Annuale sull'attività svolta nel 2020 dall'Unità d'Informazione Finanziaria, UIF, il quale attesta ancora un incremento delle segnalazioni di operazioni sospette ricevute, pari a oltre 113.000 unità, di cui quasi 2.300 relative a contesti di rischio legati all'emergenza sanitaria. Per queste ipotesi sono stati implementati gli scambi informativi sia con la Direzione Ivestigativa Antimafia (DIA), sia con le altre Financial Intelligence Unit estere (FIU), soprattutto con riguardo alle truffe telematiche (*love e romance scams, phone scams, CEO e Business Email Compromise frauds, ransomware),* alla sottrazione di fondi mediante accesso abusivo a sistemi informatici, ai pagamenti on line, anche in valute virtuali, o alle transazioni nel *dark web* connesse al traffico di stupefacenti, alla tratta di esseri umani, alla contraffazione, al commercio di materiale pedopornografico e allo sfruttamento sessuale di minori, nonché a casi sospetti di finanziamento del terrorismo. Se con riguardo a questa minaccia si tratta di fattispecie, per lo più, connotate da un basso contenuto tecnologico e organizzativo, nel 2020 diverse sono state, invece, quelle di riciclaggio connesse o a fenomeni illeciti agevolati dal massiccio ricorso, in conseguenza delle misure di distanziamento sociale e del lockdown, ai servizi telematici ed in generale alla rete, ovvero connessi alle misure di sostegno economico varate per far fronte alla crisi innescata dalla pandemia, come la distrazione degli aiuti erogati alle imprese in pagamenti on line a favore di società operanti nel settore dei giochi e delle scommesse o in investimenti mobiliari e immobiliari, anche in criptovalute.
Con riferimento a quest'ultime, si è registrato nel 2020 un incremento soprattutto delle segnalazioni riguardanti la loro associazione a fenomeni di abusivismo finanziario e truffe in *trading online,* anche da parte di soggetti che svolgono professionalmente l'attività di collettori nell'acquisto di *virtual asset*, senza però disporre di adeguate strutture organizzative e senza rispettare i presidi antiriciclaggio. Le attività di analisi, svolte in collaborazione con la CONSOB (per cui si rinvia al punto 2 di questa sezione) e le altre Autorità di vigilanza, anche estere, rilevano come le persone truffate siano adescate tramite insistenti contatti informatici o telefonici da sedicenti consulenti finanziari, che li inducono ad eseguire molteplici pagamenti di importo crescente a favore di rapporti esteri, riconducibili alle società straniere che gestiscono le piattaforme. Queste società, a loro volta, trasferiscono i fondi ad altre società e spesso tramite *Virtual Asset Service Providers*. I casi approfonditi hanno messo in luce come questi investitori possano essere truffati una seconda volta, aderendo all'offerta di consulenza legale per il recupero di quanto perduto nelle descritte operazioni di *trading* da parte di società collegate a piattaforme sospette e che richiedono ulteriori esborsi. Sempre con riferimento all'ambito dei *virtual asset* e alle truffe connesse al *trading on line,* dalle segnalazioni è risultato l'impiego, inoltre, da parte di una piattaforma di un algoritmo, basato sull'offerta/domanda di *big data* e sul traffico di dati generati e raccolti, che al fine di garantire l'incameramento di un ingiusto profitto, forzava in rialzo il prezzo delle criptovalute.
Numerosi, in ogni caso, rimangono i casi in cui l'investimento in *virtual asset* è effettuato con l'impiego di fondi illeciti, per lo più derivanti da frodi informatiche. Con riguardo a queste ipotesi desta particolare preoccupazione la diffusione del fenomeno dei c.d. "*crypto-ATM*" o ATM indipendenti, riferibili a gestori non regolamentati, sia in ambito finanziario che antiriciclaggio, costituiti da esercizi commerciali al dettaglio che consentono in contanti l'acquisto o la conversione di valute virtuali.

A queste criticità emergenti si associano quelle relative all'operatività in generale del *Virtual Asset Service Providers*. Dall'attività ispettiva eseguita su quelli operanti nel comparto italiano, costituito da quatto grandi società (una italiana e tre estere), a cui associano piccole società a responsabilità limitata con capitale minimo, emerge, in particolate, una scarsa attenzione nella profilatura della clientela, carenze nei sistemi automatici di *transaction monitoring* e l'inefficacia dei presidi inerenti al servizio di acquisto di valute virtuali mediante carte di pagamento.

Rapporto Annuale per il 2020 n. 13/2021

5. *Cybersecurity*: la lettera al mercato dell'IVASS alla luce degli Orientamenti EIOPA

Il 3 giugno 2021, l'IVASS ha fornito alcune indicazioni ai soggetti vigilati per l'adeguamento alle recenti novità previste dagli Orientamenti dell'EIOPA (l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali), dello scorso 6 aprile 2021, sulla sicurezza e sulla *governance* della tecnologia dell'informazione e comunicazione, in attuazione di quanto previsto dalla direttiva 2009/138/CE ("direttiva Solvency II") e dal regolamento delegato della Commissione 2015/35/UE.
Tra gli aspetti messi in rilievo l'IVASS indica, quali misure da implementare, con specifico riferimento al sistema di gestione dei rischi delle ICT e della *cyber security,* la determinazione di limiti di tolleranza e la predisposizione di report periodici all'Organo amministrativo, quale responsabile dell'istituzione e dell'esito del processo di gestione dei rischi. Sul piano della *governance* si segnala l'istituzione di una Funzione indipendente a cui devono essere attribuiti compiti di assistenza e *reporting* all'Organo amministrativo e di monitoraggio e coordinamento delle attività in materia di sicurezza informatica.
Sul piano di una sana gestione della continuità operativa dei sistemi ICT, conformemente al Regolamento n. 38/2018 che prevede la predisposizione di un piano, si evidenzia come sulla base degli Orientamenti bisogna procedere ad un'analisi circa l'esposizione a gravi interruzioni dell'attività e il loro potenziale impatto quantitativo e qualitativo, nonché una conseguente ideazione dell'infrastruttura ICT che tenga conto dei risultati dell'analisi.
A tal fine è richiesta l'adozione nei sistemi ICT di un processo di *change management* affinché i cambiamenti introdotti, anche quelli dovuti a situazioni emergenziali o alla mitigazione dei rischi rilevati dall'analisi, siano censiti, valutati, autorizzati e attuati in modo controllato.

Orientamenti sulla sicurezza e sulla governance della tecnologia dell'informazione e comunicazione.

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Accesso abusivo e potere ispettivi della Guardia di Finanza

Non può essere considerata abusiva ai sensi dell'art. 615-*ter* c.p. la condotta degli agenti della Guardia di Finanza, che, durante verifica fiscale, esercitando legittimamente i poteri ispettivi e di controllo loro conferiti, procedano all'accesso ad un sistema informatico mediante le relative credenziali, acquisendo anche dati informatici riferibili a società terza. Premesso che in materia di illeciti tributari sono sempre utilizzabili quale *notitia criminis* gli elementi raccolti dalla Guardia di Finanza durante gli accessi, le ispezioni e le verifiche compiuti per l'accertamento dell'imposta sul valore aggiunto e delle imposte dirette, a prescindere dalla regolarità formale della loro acquisizione, in quanto a tali attività non è applicabile la disciplina prevista dal codice di rito per l'operato della polizia giudiziaria, la società terza i cui dati informatici siano stati acquisiti in seguito a tale accesso può agire per il dissequestro solo in presenza di una pretesa giuridica, in forza della quale abbia diritto alla restituzione, ed in presenza di un decreto di sequestro probatorio che, anche laddove abbia ad oggetto cose costituenti corpo di reato, sia privo di motivazione che, per quanto concisa, dia conto specificatamente della finalità perseguita per l'accertamento dei fatti.

Per approfondire: SALVADORI I., *I reati contro la riservatezza informatica*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Torino, 2019, p. 656 ss.; FLOR R., *La condotta del pubblico ufficiale fra violazione della* voluntas domini*, "abuso" dei profili autorizzativi e "sviamento di poteri"*, in *Dir. Pen. Proc.*, 2018, n. 4, p. 506 ss.; BUSSOLATI N., *Accesso abusivo a un sistema informatico o telematico ex art. 615-ter c.p.: il nodo dell'abusività,* in *Studium iuris*, 2018, *n.* 4, p. 428 ss.; ZAMPERINI

V., *Impugnabilità del sequestro probatorio di dati informatici,* in *Diritto penale e processo*, 2016, *n.* 4, *p.* 509 ss..

Cassazione penale, sez. III penale, sentenza 25 giugno 2021, (ud. 06 maggio 2021), n. 24885/2021, Pres. Gentili- Rel. Gai

2. Detenzione di materiale pedopornografico e file cancellati

La circostanza aggravante della detenzione di ingente quantità di materiale pedopornografico di cui all'art. 600-*quater* co. 2 c.p. si configura anche nel caso in cui le immagini non siano tutte immediatamente fruibili perché cancellate o comunque accantonate, in quanto ciò che rileva è la mera detenzione di tale materiale anche per il solo tempo necessario alla sua cancellazione. In ogni caso, anche se i confini della nozione di ingente quantità non sono stati rigidamente definiti in sede normativa, si rileva che la stessa è ravvisabile ogni qual volta il numero d'immagini detenute sia significativo, a prescindere dall'effettivo numero dei *files*.

In senso conforme: Corte di cassazione, Sezione III penale, sentenza 30 agosto 2017 (ud. 26 giungo 2017), n. 39543, Pres. Savani – Rel. Di Nicola; Corte di cassazione, Sezione III penale, 31 agosto 2016, n. 35866.

Per approfondire v.: PICOTTI L., *La pedopornografia nel Cyberspace: un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale*, in *Dir. di Internet*, 2019, n. 1, p. 177 ss.; PICOTTI L., *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in M. Bertolino e G. Forti (cur.), *Scritti per Federico Stella*, Napoli, 2007, vol. II, p. 1267 ss.

Corte di Cassazione, sez. III penale, sentenza 24 giugno 2021 (ud. 3 marzo 2021), n. 24644/2021, Pres. Rosi – Rel. Gentili

3. Istigazione a pratiche di pedofilia

È stata ritenuta istigazione pubblica a commettere atti di abuso sessuale in danno di minori la pubblicazione online su dominio pubblicamente accessibile di un racconto a contenuto erotico e pedofilo contenente minuziose descrizioni e resoconti emozionali espressivi di piacere, eccitazione ed esaltazione.
Il dolo istigatorio, qualificato erroneamente dal ricorrente quale dolo specifico, configura un dolo generico coincidente con la coscienza e volontà di turbare l'ordine pubblico, da analizzarsi in relazione alla condotta, che deve ritenersi dotata di una forza suggestiva e persuasiva tale da poter stimolare nell'animo dei destinatari la commissione dei fatti criminosi propalati o esaltati, senza che questi debbano effettivamente realizzarsi.
La condotta istigatoria non esprime, sottolinea la Corte, un dolo specifico, ma concorre alla descrizione della fattispecie oggettiva connotandone la tipicità, con sfumature di natura soggettiva.
Per quanto riguarda la natura della condotta posta in essere, ossia la sua idoneità concreta a provocare un rischio effettivo di consumazione dei delitti indicati specificamente nell'art. 414-*bis* c.p., la dovizia di dettagli e la palese partecipazione e adesione dell'autore dimostrano con chiarezza la potenzialità emulativa del narrato, il quale ha suscitato diversi commenti adesivi alla storia, significativi della forza e efficacia concreta dello scritto.
A nulla rileva la circostanza che l'imputato abbia scritto a premessa del racconto l'avvertenza "l'autore crede fermamente che le molestie su minori vadano punite dalla legge nella maniera più severa".

Corte di Cassazione, sez. III penale, sentenza 18 giugno 2021 (ud. 4 maggio 2021), n. 23943/2021, Pres. Gentili – Rel. Socci

4. Adescamento di minori tramite richiesta di invio di foto erotiche via *whatsapp*

Configura il reato di adescamento di minori di cui all'art. 609-*undecies* c.p. la condotta di colui che chiede ad una dodicenne di inviargli tramite *whatsapp* fotografie ritraenti le sue parti intime, in particolare del seno e delle natiche, in quanto trattasi di raffigurazioni che ben possono essere ricomprese nella nozione di pedopornografia di cui all'art 600-*ter* c.p., poiché idonee ad eccitare l'istinto sessuale. Ai fini della fattispecie

in esame, infatti, non è necessario che la condotta contestata sia idonea alla realizzazione del reato di violenza sessuale ovvero di atti sessuali con minorenni, perché il reato di adescamento di minorenni può essere finalizzato anche alla commissione dei reati di cui agli artt. 600-*ter* e 600-*quater*, dunque anche alla mera produzione o detenzione di materiale pedopornografico.

Per approfondire: PICOTTI L., *La violenza sessuale via whatsapp*, in *Diritto di Internet*, 2020, n. 4, p. 685 ss., in commento a Corte di Cassazione, sez. III Penale, sentenza 8 settembre 2020 (ud. 2 luglio 2020), n. 25266/2020, Pres. Rosi - Rel. Macrì; SALVADORI I., *Sexting, minori e diritto penale*, in CADOPPI A., CANESTRARI S., MANNA A. e PAPA A. (a cura di), *Cybercrime*, Torino, 2019, p. 567 ss; BOGGIANI M., *L'adescamento di minorenni*, in *Cybercrime*, cit., ; p. 599 ss. PICOTTI L., *La pedopornografia nel Cyberspace: un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale riflessi nell'evoluzione normativa*, in *Diritto di Internet*, 2019, n. 1, p. 177 ss.; SALVADORI I., *I minori da vittime ad autori di reati di pedopornografia? Sui controversi profili penali del sexting*, in *Ind. pen.*, 2017, n. 3, 789 ss.; SALVADORI I., *L'adescamento di minori. Il contrasto al child-grooming tra incriminazione di atti preparatori ed esigenze di garanzia*, Torino, 2018; PICOTTI L., *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in M. Bertolino e G. Forti (cur.), *Scritti per Federico Stella*, Napoli 2007, vol. II, p. 1267 ss.

Corte di Cassazione, sez. III penale, sentenza 18 giugno 2021 (ud. 12 marzo 2021), n. 23931/2021, Pres. Marini – Rel. Gentili

5. Il dolo eventuale del *financial manager*

Non può essere considerato ignaro strumento dell'altrui attività di riciclaggio del denaro proveniente dal reato di cui all'art. 615-*ter* c.p. il soggetto che accetta una proposta di lavoro, che per contenuto e forma lessicale non può essere considerata munita di genuinità e serietà, né tantomeno lecita.
La natura illecita della "proposta di lavoro", valutata in uno con la qualità professionale dell'agente e le modalità stesse della condotta, attestano la sua consapevolezza sia della provenienza da delitto delle somme che l'imputato ha accettato di ricevere sul proprio conto corrente, sia dell'ostacolo all'identificazione della provenienza delittuosa del denaro che si realizza girando queste somme attraverso il servizio Western Union in favore di soggetti stranieri che le prelevano poi in contanti. Per la Suprema Corte, come giustamente rilevato dai giudici di merito, "*anche una persona non avvezza ad eseguire operazioni di pagamento sulla rete internet... avrebbe dovuto rendersi conto di una circostanza assolutamente evidente: e cioè della assenza di una qualche apparente utilità, in capo al proponente del fantomatico "lavoro", che non fosse quella di riciclare denaro di provenienza illecita, dell'assenza, cioè, di una qualsivoglia diversa plausibile giustificazione o ragione per la quale una fantomatica azienda multinazionale dovesse servirsi del conto corrente dell'imputato per trasferirvi pagamenti destinati a soggetti stranieri e sconosciuti*".
La possibilità che la vittima del *phishing* potesse risalire in conseguenza della tracciabilità del bonifico all'identità dell'imputato non vale ad escludere il dolo eventuale di riciclaggio, potendo essere al più indice di scarsa dimestichezza con tale tipologia di illecito o semplicemente di superficialità.

Per approfondire: FLOR R., *Phishing, identity theft e identy abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen*., n. 2-3, 2007, p. 899 ss.; ID., *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. financial manager,* in *Diritto penale e processo*, 2012, n. 1, p. 55 ss.; RAZZANTE R., *Riciclaggio e phishing. Il rischio di riciclaggio e il ruolo del financial manager secondo la Cassazione,* in *Responsabilità amministrativa delle società e degli enti (La)*, 2012, *n.* 2, *p.* 125 ss.; PIANCASTELLI S., *La ricezione di somme di denaro provento di phishing: risultanze investigative e problemi applicativi in punto di qualificazione giuridica*, in *www.dirittopenalecontemporaneo.it,* 3 marzo 2015.
Con specifico riferimento al dolo eventuale circa la provenienza illecita del provento nel vicino delitto di ricettazione cfr. Cass., Sez. Un., ud. 26.11.2009, dep. 30.3.2010, n. 12433, Nocera, pubblicata fra l'altro in *www.dirittopenalecontemporaneo.it,* 20 dicembre 2010 con commento di ABBADESSA G., *Ricettazione e dolo eventuale*.

Cassazione penale, sez. II penale, sentenza 8 giugno 2021, (ud. 09 aprile 2021), n.22475/2021, Pres. Mirella-Rel. Pellegrino

CONTRIBUTI DOTTRINALI DI RILIEVO

Braschi S., *Il ruolo delle reti sociali nel contrasto ai reati commessi all'interno del web. Tendenze evolutive e prospettive di sviluppo*, in *Rivista di Diritto dei Media*, 17 giugno 2021

Salvadori I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista italiana di diritto e procedura penale,* 2021, n. 1, p. 83 ss.

☞ **Per accedere alle newsletter dei mesi precedenti clicca qui**