News aprile 2021

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

NOVITÀ SOVRANAZIONALI

1. Il Regolamento europeo relativo al contrasto della diffusione di contenuti terroristici *online*

Prendendo atto della particolare gravità delle diffusioni in rete di contenuti di natura terroristica, le istituzioni europee hanno approvato il Regolamento 784/2021 (che si applicherà a partire dal 7 giugno 2022) volto per l'appunto a contrastare un uso improprio dei servizi di *hosting* per finalità terroristiche. Il Regolamento si fonda su una combinazione di misure legislative, non legislative e volontarie basate sulla collaborazione tra le autorità e i prestatori di servizi di *hosting*, nel pieno rispetto dei diritti fondamentali.
In particolare, il Regolamento, all'art. 3, prevede la facoltà per gli Stati membri di emettere a carico dei prestatori di servizi un ordine di rimozione di contenuti terroristici in tutti gli Stati membri. Una volta ricevuto tale ordine, gli *hosting providers* dovranno provvedere alla rimozione del contenuto il prima possibile, e in ogni caso entro un'ora dal ricevimento dell'ordine. I contenuti rimossi dovranno poi essere conservati dagli intermediari per 6 mesi ai fini delle indagini.
Inoltre, il Regolamento prevede, all'art. 5, che i prestatori di servizi di *hosting* adottino misure specifiche, efficaci e proporzionate, fondate su meccanismi automatici e automatizzati ma anche garantendo verifiche umane, laddove ritenute necessarie, per proteggere i propri servizi dalla diffusione al pubblico di contenuti terroristici. Potendo dunque i prestatori di servizi di *hosting* provvedere autonomamente alla rimozione dei contenuti ospitati sulle proprie piattaforme, il Regolamento evidenzia che, per poter garantire una tutela giurisdizionale effettiva, i fornitori di contenuti devono essere posti in grado di conoscere il motivo per cui i contenuti che essi forniscono è stato rimosso o il cui accesso è stato disabilitato. A tal fine, i prestatori di servizi di *hosting* devono mettere a disposizione del fornitore di contenuti informazioni concernenti la rimozione, nonché predisporre un meccanismo di reclamo.
In caso invece di contenuti terroristici che comportino una minaccia imminente per la vita o un presunto reato di terrorismo, quale definito dalla direttiva 541/2017, i prestatori dovranno informare tempestivamente le autorità competenti.
Gli Stati membri dovranno designare le autorità competenti (anche tra quelle esistenti) a emettere e valutare gli ordini di rimozione, controllare l'adozione delle misure specifiche, così come irrogare sanzioni. Tali autorità dovranno poi coordinarsi e cooperare tra loro a livello sovranazionale.
Vengono fatte salve disposizioni contenute nella direttiva 31/2000, per cui rimane ~~dunque~~ fermo il divieto di imporre un obbligo generale di ricerca attiva di contenuti terroristici a carico dei prestatori di servizi. Inoltre, le diverse misure adottate da questi ultimi non dovranno comportare automaticamente la perdita del beneficio dell'esenzione di responsabilità previsto in tale direttiva.
Infine, per quanto riguarda il trattamento sanzionatorio, gli Stati membri dovranno stabilire le norme relative alle sanzioni applicabili alle violazioni del Regolamento da parte dei prestatori di servizi di *hosting*, che potranno essere di natura amministrativa o penale.

Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio del 29 aprile 2021

2. *Artificial Intelligence Act*

La Commissione europea ha presentato il 21 aprile 2021 la proposta di Regolamento in materia di Intelligenza Artificiale (IA), il quale si applicherebbe a: (i) fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione Europea, indipendentemente dal fatto che tali fornitori siano stabiliti nell'Unione o in un paese terzo; (ii) utenti dei sistemi di IA che siano cittadini europei; (iii) fornitori ed utilizzatori di sistemi di IA che si trovano in un paese terzo, qualora l'*output* prodotto dal sistema sia utilizzato nell'Unione.
La presente proposta si prefigge di configurare un assetto normativo equilibrato e proporzionato, limitandosi a delineare i requisiti minimi necessari per affrontare i rischi e i problemi legati all'IA, senza limitare o

ostacolare indebitamente lo sviluppo tecnologico o aumentare in modo sproporzionato il costo di immissione sul mercato dei sistemi esperti.
La proposta stabilisce quindi regole armonizzate per lo sviluppo, l'immissione sul mercato e l'uso di sistemi di IA, seguendo un proporzionato approccio basato sul rischio. Si fornisce un'unica definizione di IA, che possa tener conto anche dei prossimi e futuri sviluppi di tali tecnologie, secondo la quale con sistema di IA deve intendersi un *software* sviluppato con una o più delle tecniche elencate nel I allegato della proposta e che può, per un dato insieme di obiettivi definiti dall'uomo, generare *output* come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono.
Alcune pratiche di IA particolarmente rischiose o dannose sono proibite in quanto contrarie ai valori dell'Unione (sono ricomprese nel Titolo II e tra queste figurano, ad esempio, le utilizzazioni di sistemi di IA che dispieghino tecniche subliminali non note agli utenti al fine di manipolarne il comportamento e causando loro un danno fisico o psicologico), mentre restrizioni e garanzie specifiche sono proposte in relazione a certe utilizzazioni dei sistemi di identificazione biometrica a distanza. La proposta stabilisce una solida metodologia per definire i sistemi di IA "ad alto rischio", che presentano rischi significativi per la salute e la sicurezza o i diritti fondamentali delle persone. Questi sistemi di IA dovranno rispettare una serie di requisiti orizzontali obbligatori per garantirne l'affidabilità, nonché seguire procedure di valutazione della conformità prima che possano essere immessi sul mercato. L'intenzione è quella di delineare obblighi prevedibili, proporzionati e chiari anche a carico dei fornitori e degli utenti di tali sistemi, per garantire la sicurezza e il rispetto della legislazione esistente durante l'intero ciclo di vita dei sistemi di IA. Per alcuni sistemi specifici, vengono proposti solo obblighi minimi di trasparenza, in particolare quando vengono utilizzati *chatbot* o "*deep fakes*".
Le regole proposte saranno applicate attraverso un sistema di *governance* a livello di Stati membri, basandosi su strutture già esistenti, e un meccanismo di cooperazione a livello di Unione con l'istituzione di un *European Artificial Intelligence Board.*

Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale (*Artificial Intelligence Act*)

2. Strategia dell'UE per contrastare la criminalità organizzata

Il 14 aprile 2021 la Commissione Europea ha presentato la Strategia quinquennale contro la criminalità organizzata, indicando specifiche azioni per contrastarne, anche, la dimensione informatica.
I crimini informatici commessi da organizzazioni criminali sono, infatti, notevolmente accresciuti nel periodo pandemico: sia per numero che per livello di sofisticazione degli attacchi *malware* e delle frodi, in particolare, con riguardo ai mezzi di pagamento diversi dai contanti. Si stima che l'80 % dei reati della criminalità organizzata abbia natura digitale e che le organizzazioni criminali sappiano usare le tecnologie informatiche e sfruttare il cyberspace per comunicare, pianificare le proprie operazioni e operare scambi di ogni tipo.
In conseguenza anche di questa particolare connotazione digitale, gli obiettivi che la Commissione si è prefissa di perseguire sono: 1. Rafforzare la cooperazione tra autorità di contrasto e autorità giudiziarie: tra le iniziative da intraprendere la Commissione proporrà di aggiornare il "quadro Prüm" per lo scambio d'informazioni su DNA, impronte digitali e immatricolazione dei veicoli, e di varare un codice unico UE di cooperazione di polizia che sostituirà l'attuale mosaico di differenti strumenti e accordi multilaterali di cooperazione; 2. Sostenere indagini più efficaci per smantellare le strutture della criminalità organizzata concentrandosi su alcuni reati specifici, per cui si ritiene sarà necessario intervenire appositamente e tempestivamente, quali, per esempio, oltre a quelli a dimensione digitale, i reati ambientali, la contraffazione di dispositivi medici e il commercio illecito di beni culturali, nonché la tratta di esseri umani, in coordinamento e connessione con la relativa strategia ad hoc già varata; 3. Garantire che il crimine non paghi: a fronte del fatto che oltre il 60 % delle reti criminali attive nell'UE agiscono attraverso la corruzione e più dell'80 % utilizzano attività commerciali legittime come facciata per le loro attività, mentre solo l'1 % dei beni di origine illecita viene confiscato, la Commissione proporrà di riesaminare il quadro dell'UE sulla confisca dei proventi di reato, la regolamentazione anticorruzione, quella antiriciclaggio, nell'ambito della quale dovrà essere mantenuta centrale l'attenzione sul mondo delle criptovalute, e quella relativa alle indagini finanziarie. 4. Avere autorità di contrasto e autorità giudiziarie pronte per l'era digitale: a tal fine il gruppo europeo di formazione e istruzione in materia di criminalità informatica svilupperà e impartirà moduli di formazione per migliorare le competenze in materia di informatica forense e criminalità informatica degli esperti delle autorità di contrasto e degli addetti al primo intervento. La Commissione finanzierà inoltre una rete di autorità di contrasto, rappresentanti del

mondo accademico e privati, che produrranno nuovi strumenti tecnologici sotto il coordinamento del laboratorio per l'innovazione di Europol. Nell'ottica di rapidità di accesso alle prove nel rispetto della tutela dei dati, viene, inoltre, promossa, la pronta partecipazione degli Stati membri al sistema digitale di scambio di prove elettroniche al fine di consentire la comunicazione elettronica sicura tra autorità giudiziarie nei casi transfrontalieri.

Comunicazione della Commissione sulla Strategia Europea per contrastare la criminalità organizzata per il 2021-2025

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Completato il processo di adesione dell'Italia alla Procura Europea

Nella Gazzetta Ufficiale, serie generale, del 1° aprile 2021 è stato pubblicato l'accordo raggiunto tra il Ministro della Giustizia, Marta Cartabia, e il Procuratore europeo, Laura Kovesi, col quale il Ministero della Giustizia ha completato la procedura di adesione dell'Italia alla Procura Europea, la cui competenza è stata determinata attraverso il rinvio alla direttiva (UE) 2017/1371 sulla protezione degli interessi finanziari dell'Unione, c.d. Direttiva PIF. L'accordo raggiunto prevede la designazione di venti Procuratori europei delegati, suddivisi tra i nove distretti di Roma, Milano, Napoli, Bologna, Palermo, Venezia, Torino, Bari e Catanzaro.

Ministero della Giustizia Accordo EPPO

2. La proroga delle misure del processo penale dell'emergenza

Con il d.l. 1 aprile 2021 n. 44, intitolato *Misure urgenti per il contenimento dell'epidemia da COVID-19, in materia di vaccinazioni anti SARS-CoV-2, di giustizia e di concorsi pubblici*, sono state prorogate al 31 luglio 2021 le disposizioni di cui al d.l. 28 ottobre 2020 n. 137, convertito con modificazioni dalla legge 18 dicembre 2020, n. 176, relative all'esercizio dell'attività giudiziaria durante l'emergenza pandemica da COVID-19. Permane, dunque, la possibilità di compiere atti d'indagine che richiedono la partecipazione della persona sottoposta alle indagini, della persona offesa, del difensore, di consulenti, di esperti o di altre persone mediante "*collegamenti da remoto"*. Inoltre, sono state prorogate le misure relative al deposito telematico degli atti nella fase delle indagini preliminari presso le procure della Repubblica, che ora costituisce modalità di deposito esclusiva per gli atti indicati dall'art. 24 d.l. 137/2020 e dal Decreto del Ministero della Giustizia del 13 gennaio 2021. Il nuovo decreto legge 44/2021 ha poi introdotto la previsione per cui il deposito degli atti "*è tempestivo quando è eseguito entro le ore 24 del giorno di scadenza*". Inoltre, all'art. 6 co. 2-bis e 2-ter è stato previsto che in caso di malfunzionamento del portale attestato dal Direttore generale per i servizi informativi automatizzati, l'autorità giudiziaria procedente può autorizzare il deposito di singoli atti e documenti in formato analogico. Tale modalità di deposito può poi essere prevista anche per "*ragioni specifiche ed eccezionali*", sempre previa autorizzazione da parte dell'autorità giudiziaria.

Per approfondire: TONDI V., *Le disposizioni del d.l. 1° aprile 2021, n. 44 in materia di procedimento penale nell'emergenza COVID-19: osservazioni a prima lettura*, in *SP*, 13 aprile 2021.

Decreto legge 1° aprile 2021, n. 44

3. I dati dei reati in rete nell'anno 2020 secondo le stime della Polizia di Stato

Nel 169° anniversario della fondazione della Polizia di Stato sono stati diffusi i dati sulla criminalità relativi al 2020, nel corso del quale, in connessione con la pandemia, il Servizio della Polizia Postale e delle Comunicazioni è stato impegnato in una capillare attività di monitoraggio dei *social network* e della Rete volta alla prevenzione e al contrasto di fenomenologie criminali come cyberbullismo, pedopornografia e truffe.

Nello specifico, sotto il coordinamento del Centro Nazionale per il Contrasto della Pedopornografia online sono stati analizzati i contenuti di 34.120 siti internet con l'inserimento di 2.446 spazi web illeciti nella *black list* per inibirne l'accesso dal territorio italiano ed è stato registrato un incremento significativo dei casi di adescamento di minori online d'età compresa tra 0-9 anni.
Nel contesto dei *social network* numerosi sono stati i casi trattati di estorsioni a sfondo sessuale, *revenge porn*, *stalking*, molestie, minacce, ingiurie e diffamazione online.
Significativa è stata anche l'azione di contrasto alle *fake news*, ai reati d'incitamento all'odio, con particolare attenzione per gli atti intimidatori posti in essere nei confronti dei giornalisti, e alla propaganda islamica con oltre 37.000 spazi web visionati.
Con riferimento ai reati contro il patrimonio, in continua crescita risultano i dati relativi alle truffe online e specificatamente quelle legate al *trading* online con oltre 20 milioni di euro sottratti alle vittime. Relativamente al *financial cybercrime,* su 4.294 casi nazionali, nonostante il dirottamento delle somme frodate verso Paesi extraeuropei, grazie alla piattaforma *On line fraud cyber centre and expert network* la Polizia Postale e delle Comunicazioni ha potuto recuperare alla fonte 20.046.240,51 euro, su una movimentazione complessiva di 33.186.673,91 euro.
Con riferimento alla *cybersecurity*, la Sala Operativa del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche ha gestito, a livello nazionale, 509 attacchi a sistemi informatici di strutture nazionali di rilievo strategico, 69 richieste di cooperazione nel circuito *High Tech Crime Emergency* e avviato 103 indagini con 105 persone indagate.

PoliziaModerna-dati 2020

4. Avvertimento del Garante privacy sul Decreto "Riaperture" per i pass vaccinali

Con un avvertimento formale, adottato ai sensi del Regolamento Ue 2016/679, il Garante ha richiamato il Governo sulle criticità del sistema previsto dal Decreto cd. "riaperture" del 22 aprile 2021, n. 52, per la creazione e la gestione delle "certificazioni verdi", i cosiddetti pass vaccinali.
Si rappresenta, prima di tutto, come il decreto legge non costituirebbe una valida base giuridica per l'introduzione e l'utilizzo dei certificati verdi a livello nazionale, essendo privo di alcuni degli elementi essenziali richiesti dal Regolamento (artt. 6, par. 2 e 9) e dal Codice in materia di protezione dei dati personali (artt. 2 *ter* e 2 *sexies*).
Si contesta, inoltre, la mancata consultazione del Garante, nonostante l'introduzione delle "certificazioni verdi" generi un trattamento sistematico di dati personali, anche relativi alla salute, su larga scala, che presenta un rischio elevato per i diritti e le libertà degli interessati: in contrasto con quanto previsto dal Regolamento europeo in materia di protezione dei dati personali, il decreto non definirebbe né le finalità del trattamento dei dati sulla salute degli italiani, lasciando spazio a molteplici e imprevedibili utilizzi futuri, né chi ne sarebbe il titolare, impedendo di fatto l'esercizio dei diritti degli interessati. Il sistema come delineato dalle disposizioni normative del decreto comporterebbe, anche, un utilizzo eccessivo di dati sui certificati da esibire in caso di controllo, in violazione del principio di minimizzazione, e il rischio, soprattutto nella fase transitoria, di dati inesatti o non aggiornati con gravi effetti sulla libertà di spostamento individuale. Non sarebbero nemmeno previsti tempi di conservazione dei dati né misure adeguate a garantire la loro integrità e riservatezza.
Alla luce dell'operatività delle certificazioni verde a partire dal giorno successivo alla pubblicazione del decreto legge, il Garante avverte della necessità di intervenire urgentemente sulle diverse criticità segnalate al fine di tutelare i diritti e le libertà degli interessati.

Provvedimento di avvertimento in merito ai trattamenti effettuati relativamente alla certificazione verde per COvid-19 prevista dal d.l. 22 aprile 2021, n. 52 - 23 aprile 2021

5. Consob e Banca d'Italia mettono in guardia contro i rischi insiti nelle cripto-attività

Facendo seguito all'avvertimento diramato a marzo 2021 dalle tre Autorità europee di vigilanza - Eba, Esma ed Eiopa - e tenuto conto che è attualmente in corso l'iter per l'approvazione della proposta della Commissione Europea (consultabile al Topic *FinTech*) di regolamentazione e contrasto agli abusi di mercato in relazione

alle diverse tipologie di cripto-attività, congiuntamente Banca d'Italia e Consob in data 28 aprile 2021 hanno richiamato, soprattutto i piccoli consumatori, sugli elevati rischi connessi agli investimenti in questi strumenti. Questi rischi, che possono determinare la perdita integrale del denaro investito, derivano, da un lato, dal fatto che le cripto-attività non sono soggette alle norme in materia di trasparenza dei prodotti bancari e dei servizi di investimento, nonché a nessuna forma di supervisione o di controllo da parte delle Autorità di vigilanza, dall'altro, dalla loro natura e circolazione digitale.
Nello specifico appartengono alla prima categoria la scarsa disponibilità di informazioni in merito alle modalità di determinazione dei prezzi, la volatilità delle quotazioni, l'assenza di obblighi informativi e di tutele legali e contrattuali, a salvaguardia, in particolare, delle somme impiegate. Ineriscono, invece, alla seconda tipologia i malfunzionamenti delle tecnologie sottostanti, gli attacchi informatici ai relativi operatori e ancora la perdita/smarrimento delle credenziali di accesso ai portafogli elettronici.
È indicata come altrettanto rischiosa, anche, l'adesione a offerte di prodotti finanziari correlati a cripto-attività, come i cd. *digital token*, a maggior ragione quando effettuata da operatori abusivi, non autorizzati e non vigilati da alcuna Autorità.

Comunicato stampa congiunto Consob-Banca d'Italia 28 aprile 2021

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Diffamazione via Internet e proporzionalità del trattamento sanzionatorio

La Corte di Cassazione ha disposto l'annullamento della sentenza impugnata limitatamente al trattamento sanzionatorio di 4 mesi di detenzione irrogato per una diffamazione commessa mediante pubblicazione di post denigratori su Facebook, in quanto contraria alla giurisprudenza della Corte Edu.
Sulla base di quest'ultima, in conseguenza della sussistenza del rischio di effetto dissuasivo *(chilling effect*) dell'esercizio del diritto, al di fuori anche dell'ambito dell'attività giornalistica, la pena detentiva per diffamazione è compatibile con la libertà di espressione garantita dall'art. 10 CEDU soltanto in circostanze eccezionali, qualora siano stati lesi gravemente altri diritti fondamentali, come, per esempio, in caso di discorsi di odio o di istigazione alla violenza.
L'annullamento della sentenza gravata è operata dalla Suprema Corte richiamando anche la giurisprudenza costituzionale ed, in particolare, l'ordinanza n. 131 del 2020 della Corte Costituzionale, che ha evidenziato la necessità di una rimeditazione del bilanciamento tra libertà di manifestazione del pensiero e tutela della reputazione conformemente alla "*rapida evoluzione della tecnologia e dei mezzi di comunicazione"* e agli "*effetti di rapidissima e duratura amplificazione degli addebiti diffamatori determinata dai social networks e dai motori di ricerca in Internet"*, a prescindere dall'esercizio dell'attività giornalistica.
In generale relativamente al profilo costituzionale, la Corte di Cassazione ritiene che escludere la pena detentiva – riservandola soltanto ai c.d. discorsi d'odio – alle sole ipotesi di diffamazione commessa nell'esercizio dell'attività giornalistica, rischi di compromettere, da un lato, il principio di uguaglianza nei confronti di tutti i cittadini e, dall'altro, il principio di ragionevolezza, prevedendo un trattamento sanzionatorio sfavorevole per fatti di solito connotati da minore gravità e/o diffusività rispetto a quelli commessi nell'esercizio dell'attività giornalistica.

Per approfondire: PISAPIA M., CHERCHI C., *Detenzione e libertà di espressione. Riflessioni sul trattamento sanzionatorio del reato di diffamazione a mezzo stampa in occasione della pronuncia della Corte Costituzionale*, in *Giurisprudenza penale*, 2020, n. 6, p. 1 ss.; UBIALI M., *Diffamazione a mezzo stampa e pena detentiva: la Corte costituzionale dà un anno di tempo al Parlamento per trovare un punto di equilibrio tra libertà di espressione e tutela della reputazione individuale, in linea con i principi costituzionali e convenzionali*, nota a Corte Costituzionale, ordinanza 26/06/2020, n. 132, in *Rivista italiana di diritto e procedura penale*, 2020, n. 3, p. 1476 ss.; BRANCACCIO M., *Libertà di espressione e diritto di cronaca: l'intervista, l'interesse pubblico all'informazione e i confini della diffamazione*, nota a Corte europea dei diritti umani, sez. I, sentenza 16/01/2020, n. 59347, in *Cassazione penale*, 2020, n. 11, p. 4341 ss.; CUCCHIARA

M., *Diffamazione, Libertà di espressione e Diritto alla vita privata: un delicato bilanciamento*, in *Giurisprudenza penale*, 2017, n. 2, p. 1 ss; PETRINI D., *Diffamazione on line: offesa recata con "altro mezzo di pubblicità" o col mezzo della stampa?*, in *Diritto penale e processo*, 2017, n. 11, p. 1485 ss; GARUTI G., *Libertà di espressione e delitto di diffamazione*, in *Diritto penale e processo*, 2010, n. 3, p. 377 ss..

Corte di Cassazione, Sez. V penale, sentenza 14 aprile 2021 (ud.17 febbraio 2021), n. 13993/2021, Pres. Sabeone - Rel. Riccardi

2. Post diffamatorio via Facebook e scriminante del diritto di critica

Per la Corte di Cassazione, ancorché in tema di diffamazione l'esimente del diritto di critica non vieti l'utilizzo di termini che, sebbene oggettivamente offensivi, siano insostituibili nella manifestazione del pensiero critico, l'uso della qualificazione di "essere spregevole" nei confronti del collega, associata all'accusa di "manipolazioni psicologiche" nei confronti degli studenti, travalica il limite della continenza ed è idonea a ledere la dignità professionale di un insegnante. Il senso della parola in sé e nel contesto fattuale di riferimento, non può che essere quello di attribuire all'insegnante, per ragioni neppure manifestate o circostanziate, una volontà di condizionamento/controllo delle coscienze dei suoi studenti, volontà che appare, all'evidenza, contraria agli scopi formativi ed educativi che l'ordinamento attribuisce all'insegnamento.
Integra, pertanto, il reato di diffamazione aggravato ai sensi dell'art. 595, comma 3 c.p., la diffusione di un messaggio diffamatorio di tale fatta attraverso l'uso di una bacheca Facebook, costituente "mezzo di pubblicità" potenzialmente capace di raggiungere un numero indeterminato, o comunque quantitativamente apprezzabile, di persone.

Per approfondire: ALBAMONTE E., *La diffamazione a mezzo web*, in PARODI C. (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, 2020, p. 487 ss.; LASALVIA F. P., *La diffamazione via web nell'epoca dei social network*, in CADOPPI A., CANESTRARI S., MANNA A. e PAPA A. (a cura di), *Cybercrime,* Torino, 2019, p. 331 ss.; AMERIO L., *Offendere su Facebook? È diffamazione aggravata*, in *Giurisprudenza penale*, 2016, n. 3, p. 1 ss.; CORBETTA, *Offese all'altrui onore postate su facebook: è diffamazione aggravata*, in *Diritto penale e processo*, 2016, n. 4, p. 464 ss.; ALMA R., *La pubblicità di un messaggio diffamatorio su Facebook integra il delitto di diffamazione aggravata*, in *Diritto dell'informazione e dell'informatica*, 2013, n. 3, p. 518 ss.

Corte di Cassazione, Sez. V penale, sentenza 14 aprile 2021 (ud. 25 gennaio 2021), n. 13979/2021, Pres. Sabeone – Rel. De Gregorio

3. Diffamazione via mail: le nozioni di "presenza" e "distanza"

Poiché le e-mail non sono altro che lettere in formato elettronico recapitate dalla casella di posta elettronica del mittente a singoli destinatari, non contestualmente presenti, è ravvisabile il delitto di cui all'art. 595 c.p. nel caso di invio di una e-mail, dal contenuto offensivo, destinata sia all'offeso sia a più di due persone. La nozione di "presenza" dell'offeso implica necessariamente la presenza fisica, in unità di tempo e di luogo, di offeso e spettatori ovvero una situazione ad essa sostanzialmente equiparabile realizzata con l'ausilio dei moderni sistemi tecnologici come *call conference*, audio conferenza o videoconferenza. Ne deriva che in caso di offesa proferita nel corso di una riunione "a distanza" (o "da remoto"), tra più persone contestualmente collegate, alla quale partecipa anche l'offeso, ricorrerà l'ipotesi della ingiuria commessa alla presenza di più persone (fatto depenalizzato); di contro, laddove vengano in rilievo comunicazioni (scritte o vocali), indirizzate all'offeso e ad altre persone non contestualmente "presenti", ricorreranno i presupposti della diffamazione.

Per approfondire: ALBAMONTE E., *La diffamazione a mezzo web*, in PARODI C. (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, 2020, p. 487 ss.; CORBETTA S., *Quando si realizza la diffamazione commessa mediante invio di e-mail*, in *Diritto penale e processo*, 2019, n. 2, p. 204 ss.; LASALVIA F. P., *La diffamazione via web nell'epoca dei social network*, in CADOPPI A., CANESTRARI S., MANNA A. e PAPA A. (a cura di), *Cybercrime,* Torino, 2019, p. 331 ss.; GIACHELLO E., *La diffamazione su Facebook: un reato generazionale e un dilemma interpretativo*, in *Giurisprudenza penale*,

2018, n. 9, p. 1 ss.; CORBETTA S., *Offesa dell'onore altrui in una chat vocale: ingiuria o diffamazione?*, nota a Cassazione penale, sez. V, sentenza 31/03/2020, n. 10905, in *Diritto penale e processo*, 2020, n. 5, p. 618 ss.; LA ROSA E., *Offese in videochat: la Corte di Cassazione si pronuncia sui rapporti tra ingiuria e diffamazione*, in *Giurisprudenza italiana*, 2020, n. 7, p. 1750 ss.; PIOLETTI U., *Ingiuria, diffamazione e reti sociali*, in *Giurisprudenza di merito*, 2012, n. 12, p. 2652 ss..

Corte di Cassazione, Sez. V penale, sentenza 8 aprile 2021 (ud. 4 marzo 2021), n. 13252/2021, Pres. Palla - Rel. Morsini

4. Accesso abusivo al "cassetto fiscale" altrui

Il "servizio informatico fiscale", definito cassetto fiscale, rientra nell'alveo della nozione di domicilio informatico, alla cui inviolabilità è diretta la tutela penale del precetto previsto dall'art. 615-*ter* c.p.. Commette pertanto il reato di accesso abusivo il soggetto che si introduce nel cassetto fiscale di una persona, nel caso di specie un familiare, utilizzando indebitamente password ottenute in vece del titolare, senza il suo consenso, ignorando deliberatamente la volontà palese della persona offesa di revocare la delega di agire in sua vece prima concessa all'autore del reato.
Specifica inoltre la Corte di Cassazione che, in ambito di relazioni private ed endofamiliari, ai fini della configurabilità del reato *ex* art. 615-*ter* c.p., non rileva la circostanza che le chiavi di accesso al sistema informatico protetto siano state comunicate dal titolare all'autore del reato in epoca antecedente rispetto all'accesso abusivo, qualora la condotta incriminata abbia portato ad un risultato certamente in contrasto con la volontà della persona offesa ed esorbitante l'eventuale ambito autorizzatorio.
Viene dunque affermato il seguente principio di diritto: "configura il reato previsto dall'art. 615-*ter* c.p. la condotta di chi si introduca nel cassetto fiscale altrui, contenuto nel sistema informatico dell'Agenzia delle Entrate, utilizzando password modificate e contro la volontà del titolare".

In senso conforme: Corte di Cassazione, Sez. Un., sentenza 8 settembre 2017 (ud. 18 maggio 2017), n. 41210/2017, Pres. Canzio – Rel. Saviani; Corte di Cassazione, Sez. Un., sentenza 7 febbraio (ud. 27 ottobre 2011), n. 4694/2011, Pres. Lupo – Rel. Fiale.

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.; ID., *Quando un insider accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615-ter c.p.*, in *Riv. Trim. Dir. Pen. Economia,* 2012, p. 369 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..

Corte di Cassazione, Sez. V penale, sentenza 27 aprile 2021 (ud. 15 febbraio 2021), n. 15899/2021, Pres. Palla – Rel. Brancaccio

5. Istigazione al suicidio e *social networks*

Il giudice per le indagini preliminari del Tribunale di Milano ha disposto l'archiviazione del procedimento aperto a seguito della tragica scomparsa di un minore di quattordici anni, rinvenuto privo di vita per aver provato ad emulare la cosiddetta "sfida del *blackout*", basata sulla volontaria adozione di tecniche di soffocamento, finalizzate a provocare una transitoria perdita di coscienza e una sensazione di "ebbrezza". Il minore, eseguendo su sé stesso la tecnica di soffocamento, dopo aver visionato il video sulla rete, è rimasto in questo modo vittima di un tragico incidente.
In particolare, il video visionato dal minore era un video caricato sul portale YouTube, dal titolo "5 *Challenge* pericolosissime che i ragazzi fanno per internet", in cui venivano descritte cinque pratiche estremamente pericolose messe in atto dai ragazzi per riprendersi e "postare" i video sulla rete e in cui lo stesso autore raccomandava di non imitare tali gesti, evidenziandone la pericolosità.
Secondo il GIP, per quanto riguardava la configurabilità del reato di cui all'art. 580 c.p., dalla descrizione dei fatti non si evincevano sufficienti principi di prova per sostenere l'accusa in giudizio, in primo luogo per difetto di dolo. Non è stato individuato infatti l'elemento soggettivo di far sorgere, rafforzare o agevolare il proposito suicidiario nella indistinta platea degli utenti della rete internet, dal momento che il video evidenziava più volte

l'alto pericolo di tali "sfide", avvertendo ripetutamente di non sperimentarle. Inoltre, non sono stati ritenuti sussistenti gli elementi costitutivi della condotta descritta dalla fattispecie di cui all'art. 580 c.p., dal momento che nel caso di specie non era rinvenibile alcuna volontà suicidaria da parte del minore (né questa era stata dunque determinata, agevolata o rafforzata).
Per quanto riguardava invece il reato di omicidio colposo, dal momento che gli autori del video (realizzato due anni prima della verificazione della tragica morte del giovane) spiegavano con estrema chiarezza la natura assolutamente rischiosa delle condotte descritte, non è stato ritenuto configurabile, non essendovi profili di colpa nella condotta degli indagati, né un nesso di causalità tra le eventuali condotte e l'evento morte per come concretamente verificatosi.

Decreto di archiviazione del 21 marzo 2021, G.I.P. Tribunale di Milano

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

CROCE M., Cyberlaundering *e valute virtuali. La lotta al riciclaggio nell'era della* distributed economy.

DELLA TORRE J., *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*

RIVA E., *Le fattispecie di danneggiamento informatico: una comparazione tra Italia e Cina.*

Altre riviste

PIERGALLINI C., *Intelligenza Artificiale: da 'mezzo' ad 'autore' del reato?*, in *Riv. it. dir. proc. pen.,* 2020, n. 4, p. 1745 ss.

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