News novembre - dicembre 2021

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

NOVITÀ SOVRANAZIONALI

1. Proposta Commissione Europea estensione dei reati previsti dall'art. 83 TFUE

In data 9 dicembre 2021, in continuità con le azioni già intraprese nel contrasto dei contenuti d'odio online, la Commissione Europea ha presentato la **proposta d'inserimento dei reati d'incitamento all'odio nell'elenco delle forme di criminalità gravi e transnazionali**, per cui l'Unione può, ai sensi dell'articolo 83, paragrafo 1, TFUE, stabilire mediante direttive norme minime relative ai delitti e alle sanzioni applicabili.
Il predetto ampliamento viene giustificato in virtù sia del **carattere transnazionale di questi reati** conseguente, in particolare, alla loro realizzazione e diffusione online, sia quale **forma di criminalità particolarmente grave fondata sull'"odio"** nei confronti di specifici soggetti o gruppi di persone, quali donne, rom, disabili, **in contrasto con i valori comuni dell'UE**, i diritti fondamentali sanciti dagli articoli 2 e 6 del trattato sull'Unione europea, nonché dalla Carta europea dei diritti fondamentali.
All'omogeneità di questi reati con quelli già contemplati dall'art. 83 TFUE, la Commissione aggiunge **l'impellenza d'intervenire** generata, da un lato, dall'incremento della loro realizzazione favorito dall'evoluzione economica, sociale e tecnologica innescata dalla pandemia da COVID-19, dall'altra, dalle differenze regolamentari esistenti tra gli Stati membri nonostante gli sforzi profusi nell'attuare la decisione quadro del Consiglio sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale.
Affinché la proposta abbia seguito il Consiglio dovrà adottare all'unanimità, previa approvazione del Parlamento europeo, una decisione che identifichi l'incitamento all'odio e i reati generati dall'odio come altra sfera di criminalità rispondente ai criteri di cui all'articolo 83, paragrafo 1, TFUE e solo in seguito la Commissione potrà presentare le relative proposte di direttive.

Communication from the Commission to the European Parliament and the Council. A more inclusive and protective Europe: extending the list of EU crimes to hate speech and hate crime

2. Rapporto annuale della Commissione Europea sull'applicazione della Carta dei diritti fondamentali dell'Unione

In attuazione della Strategia per rafforzare l'applicazione della Carta dei diritti fondamentali dell'Unione Europea del 2020, la Commissione europea ha pubblicato **la prima relazione annuale**. Il predetto rapporto si concentra, in particolare sulle **sfide proprie dell'era digitale**, affrontando **cinque aspetti chiave**: **il primo** riguarda i **rischi connessi**, non solo per il confronto democratico, **alla diffusione di contenuti illegali su Internet**; **il secondo** attiene **all'utilizzo dell'intelligenza artificiale**, il quale pur generando grandi vantaggi ed essendo stato oggetto di strategie nazionali apposite per garantirne trasparenza, continua ad essere una sfida per il rispetto o l'applicazione dei diritti fondamentali; **il terzo** attiene al **superamento del divario digitale accentuato dalla pandemia da COVID-19**; **il quarto** riguarda **la protezione dei lavoratori in smart working** o che si avvalgono di piattaforme per il lavoro a distanza; **il quinto** concerne **la supervisione della sorveglianza digitale** in quanto quest'ultima, pur potendo essere legittima per contrastare la criminalità e garantire la sicurezza, può comportare pratiche abusive in pregiudizio della protezione dei dati e della privacy, i quali costituiscono diritti fondamentali essenziali per la garanzia di altri diritti. La Commissione ha invitato il Parlamento europeo, il Consiglio e gli Stati membri a utilizzare la relazione nel dialogo per l'elaborazione di soluzioni condivise.

Annual report commissione diritti fondamentali era digitale 10 dicembre 2021

3. Le indicazioni del Parlamento Europeo nel contrasto alla violenza di genere on line

A seguito di un dibattito in plenaria, il 14 dicembre il Parlamento Europeo ha adottato **il progetto di iniziativa legislativa**, presentato dalle commissioni per i diritti delle donne e le libertà civili, **per combattere la cyber-violenza di genere**, drammaticamente aumentata nel corso della pandemia da COVID-19, e conseguire un livello minimo di protezione e riparazione per le vittime, in linea con gli standard stabiliti nella Convenzione di Istanbul.

Il progetto approvato, partendo dalla considerazione che **la violenza informatica contro le donne e le persone LGBTIQ è una continuazione della violenza di genere offline**, richiede che siano **contrastati con urgenza e in maniera armonizzata fenomeni come lo stalking informatico, le violazioni della privacy**, attuante anche mediante sistemi di controllo o sorveglianza a distanza, come le app spia, **l'incitamento all'odio sessista, l'induzione all'autolesionismo, la registrazione e la condivisione di immagini di aggressioni sessuali**. Si chiede, oltre all'adozione di una direttiva che fornisca una definizione comune agli effetti del diritto penale di cyber violenza di genere, che **il Consiglio riconosca ufficialmente la violenza di genere come un crimine particolarmente grave a dimensione transfrontaliera ai sensi dell'art. 83 del TFUE**.

Gender-based cyberviolence: Parliament calls for EU law to tackle the problem

4. La Corte EDU e il bilanciamento tra il diritto alla reputazione, la libertà di stampa e il diritto alla protezione dei dati personali

La Corte Europea dei diritti dell'Uomo ha precisato che **l'anonimato degli utenti** che lasciano commenti sul sito *web* di un quotidiano non è un diritto assoluto, ma **dev'essere comunque tutelato** per garantire la libertà di stampa, cruciale per il dibattito su questioni di interesse pubblico. Pertanto, i giudici nazionali non possono pretendere che una testata *online* riveli i dati personali degli utenti registrati per i commenti pubblicati sul sito senza compiere un bilanciamento dei diritti in gioco, considerando che proprio **l'anonimato sul *web* favorisce la libera circolazione di opinioni, idee e informazioni**. La Corte Europea dei diritti dell'Uomo, dunque, ha condannato lo Stato austriaco per aver ordinato ad una società editoriale di consegnare i dati personali di due utenti registrati che avevano commentato una notizia di cronaca contenuta sul sito relativa ad un leader politico regionale definendo quest'ultimo neonazista. Per i giudici europei, sebbene **l'anonimato su *internet* non sia un diritto assoluto**, le autorità nazionali, prima di ordinare l'esecuzione di una misura relativa alla divulgazione dei dati personali degli utenti, devono comunque effettuare un **bilanciamento tra i diritti e gli interessi in gioco**, ovvero il diritto alla reputazione, da una parte, e la libertà di stampa ed il diritto alla protezione dei dati personali. In questo caso la divulgazione dei dati di questi utenti è stata considerata una **misura sproporzionata**, perché **tale da scoraggiare questi ultimi a partecipare ad un dibattito e condividere le proprie idee e opinioni**, diritti tutelati sia dalla libertà di stampa che da quella di espressione.

Corte europea dei diritti dell'uomo, 7 dicembre 2021, app. n. 39378/2015 Standard Verlagsgesellschaft MBH c. Austria

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Il d.lgs. 8 novembre 2021, n. 184 di attuazione della Direttiva 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti

È stato pubblicato nella Gazzetta ufficiale n. 284 del 29 novembre 2021 il **d.lgs. 8 novembre 2021 n. 184 di attuazione della Direttiva 2019/713/UE dedicata alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti** (cfr. News OC luglio – agosto 2021). Tale decreto ha apportato alcune modifiche al codice penale. In particolare, è stato **modificato l'art. 493-*ter* c.p.**, ora rubricato "indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti", il cui **oggetto del reato è stato ampliato sino a ricomprendere tutti gli strumenti di pagamento diversi dai contanti**. All'**art. 493-*quater* c.p.** è stato

introdotto **il nuovo delitto di "detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti"**. Tale nuova fattispecie sanziona chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o ad altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo. Inoltre, **all'art. 640-*ter* c.p.**, è stata introdotta una **nuova circostanza aggravante ad efficacia speciale per il caso in cui si sia effettivamente verificato un "*trasferimento di denaro, di valore monetario o di valuta virtuale*"**. Il decreto fornisce poi le definizioni, ai fini della legge penale, di "strumento di pagamento diverso dai contanti", di "dispositivo, oggetto o record protetto", di "mezzo di scambio digitale" e di "valuta virtuale". È stata poi modificata la **disciplina relativa alla confisca**, prevedendo che in caso di condanna o patteggiamento sia sempre disposta la confisca delle apparecchiature, dei dispositivi e dei programmi informatici utilizzati per commettere i reati menzionati. Infine, il decreto ha inciso anche sulla **responsabilità da reato degli enti**, introducendo **il nuovo articolo 25-*octies*.1**, che sanziona l'ente nel cui interesse o vantaggio sono stati commessi i reati di cui agli artt. 493-*ter* c.p., 493-*quater* e 640-*ter* c.p. aggravato dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale. Inoltre, **al co. 2 dell'art. 25-*octies*.1 cit. è stato previsto un nuovo illecito amministrativo sussidiario** in caso di commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, avente ad oggetto strumenti di pagamento diversi dai contanti.

Per approfondire: VADALÀ R.M., *La tutela penale della sicurezza degli scambi economici digitali*, Università degli Studi di Verona, Dipartimento di Scienze Giuridiche, formato ebook-cod. ISBN 9788899957025, ottobre 2021; VADALÀ R.M., *La disciplina penale degli usi e abusi delle valute virtuali*, in *Dir. di Internet*, 2020, n. 3, p. 379 ss.

D.lgs. 8 novembre 2021, n. 184 di attuazione della Direttiva 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti

2. Norme integrative per i giudizi davanti alla Corte costituzionale: avvio del portale *e-Cost*

Con Decreto del 28 ottobre 2021 del Presidente della Corte Costituzionale sono state previste le modalità attuative per l'**introduzione del Processo Telematico anche presso la Corte Costituzionale**. Il **portale *e-Cost*** è entrato in funzione il 3 dicembre 2021 ed è ora operativo. Tramite lo stesso portale è possibile caricare gli atti e i documenti da inoltrare alla Corte, consultare lo stato del fascicolo e scaricare atti e documenti depositati dalle altre parti. L'**obbligatorietà del deposito telematico** vale solo per i giudizi il cui atto introduttivo sia di data successiva al 3 dicembre 2021. Il decreto specifica poi che i file caricati debbono necessariamente essere in formato .pdf oppure .p7m e che per tutto quanto non specificamente previsto si rimanda alla normativa in materia di Processo Amministrativo Telematico. Per quanto riguarda invece i termini, si specifica che ai fini del computo dei termini, la data di deposito corrisponde alla data di inserimento nel sistema e non alla data di verifica da parte della cancelleria e che il termine è rispettato se l'atto viene inserito nel sistema entro le ore 24,00 del giorno di scadenza.

Decreto del Presidente della Corte costituzionale del 28 ottobre 2021

3. Convertito in legge il decreto legge n. 132/2021 in materia di *data retention*

La **legge 23 novembre 2021, n. 178 ha convertito in legge il decreto legge n. 132/2021**, che ha modificato la disciplina dell'art. 132 del d.lgs. 196/2003 (codice *privacy*) in materia di *data retention*, allo scopo di adeguare la legislazione nazionale ai principi enunciati dalla Corte di giustizia nella sentenza 2 marzo 2021 (cfr. News OC settembre-ottobre 2021). Il decreto legge ha limitato la possibilità di acquisire i dati relativi al traffico telefonico e telematico ai procedimenti riguardanti i soli reati per i quali la legge stabilisce la pena

dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, nonché i reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo siano gravi.
Il testo del decreto legge è stato modificato in alcune parti dalla legge di conversione. Tra le **novità maggiormente significative** si segnalano quelle riguardanti l'articolo 1, al cui primo comma si vincola la rilevanza che devono assumere i dati acquisiti non più alla prosecuzione delle indagini, dal momento che l'espressione «… ove rilevanti ai fini della prosecuzione delle indagini» è **stata sostituita dall'espressione «...ove rilevanti per l'accertamento dei fatti»**. La **previgente dicitura è stata infatti ritenuta troppo limitativa**, poiché la necessità di acquisire i tabulati si può porre, anche se meno frequentemente, anche dopo l'esercizio dell'azione penale, davanti al giudice del dibattimento.
Inoltre, sempre al primo comma l'inciso «...i dati sono acquisiti presso il fornitore con decreto motivato del giudice su richiesta...» è stato **sostituito dalla seguente formulazione: «i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero»**, fugando così ogni dubbio riguardante l'idea di un giudice dotato di poteri acquisitivi diretti, seppur veicolati dalle parti.
Viene inoltre **inserito all'art. 132 del codice privacy un nuovo comma 3-*quater*, secondo cui «i dati acquisiti in violazione delle disposizioni dei commi 3 e 3-*bis* non possono essere utilizzati»**.
Infine, con riguardo alle **questioni di diritto intertemporale** connesse all'utilizzabilità (ovvero all'eccepita inutilizzabilità in sede di ricorso per cassazione) dei dati acquisiti precedentemente e al di fuori delle condizioni fissate dalla novella legislativa, si introduce anche il comma 1-*bis* all'art. 1 del decreto legge n. 132, secondo cui i dati acquisiti nei procedimenti penali in data precedente alla data di entrata in vigore del decreto possono essere utilizzati a carico dell'imputato solo unitamente ad altri elementi di prova ed esclusivamente per l'accertamento dei reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, e dei reati di minaccia e di molestia o disturbo alle persone con il mezzo del telefono, quando la minaccia, la molestia o il disturbo sono gravi.

Legge 23 novembre 2021, n. 178 e relazione n. 67/2021 a cura dell'Ufficio del Massimario e del Ruolo della suprema Corte di Cassazione

4. Divieto di installazione ed utilizzo di sistemi di riconoscimento facciale

Il **decreto legge 8 ottobre 2021, n. 139, è stato convertito in legge, con modificazioni, dalla legge 3 dicembre 2021, n. 205**. In particolare, i commi da 9 a 12 dell'articolo 9 del decreto legge sono **dedicati alla disciplina della protezione dei dati personali, disponendo una sospensione** (eccezion fatta per la prevenzione e la repressione dei reati) **della installazione e utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici in luoghi pubblici o aperti al pubblico, da parte di autorità pubbliche o soggetti privati**. Tale moratoria è prevista "fino all'entrata in vigore di una disciplina legislativa della materia", e comunque non oltre il 31 dicembre 2023. La violazione della moratoria comporta l'applicazione di sanzioni amministrative pecuniarie, salvo che il fatto costituisca reato.

Legge 3 dicembre 2021, n. 139.

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Partecipe all'associazione con finalità di terrorismo

Con riferimento al **delitto di associazione con finalità di terrorismo**, **la partecipazione all'ISIS** o ad analoghe associazioni internazionali, rispondenti ad un modello "polverizzato" di articolazione, **può essere desunta da concrete condotte sintomatiche della condivisione ideologica delle finalità dell'associazione e della messa a disposizione del partecipe**, non implicanti necessariamente una formale accettazione da parte del gruppo terroristico, ma attestanti contatti con i livelli intermedi o propaggini finali, anche "mediatamente"

e flebilmente riconducibili alla "casa madre", purché idonei a dare una qualche consapevolezza, anche indiretta, della sua adesione.
Nel caso deciso la Corte ha reputato esente da censure il giudizio del Giudice di merito che aveva attribuito rilevanza, quali elementi di fatto da cui desumere il contributo materiale e funzionale prestato dal partecipe ai fini della realizzazione delle finalità del sodalizio, alle **numerose fotografie reperibili on line dell'imputato ritratto insieme ad altri militanti/combattenti nell'intento di compiere un gesto (il dito indice alzato) di incitamento alla jihad, ed alla sua attività di proselitismo realizzata tramite Facebook**.
Nello specifico, mediante il social network, l'imputato aveva diffuso non solo i segni del cambiamento fisico e spirituale in seguito alla conversione, ma anche immagini della esecuzione di ostaggi e di predicatori che glorificavano atti violenti, accompagnati da scritte inneggianti alla lotta armata.

Per approfondire: AMATO G., *Terrorismo internazionale: per la 'partecipazione' occorre che l'associazione lo sappia e ci possa contare*, in *Guida al diritto*, 2019, n. 6, p. 82 ss.; TIANI E., *La responsabilità oggettiva in relazione all'età della persona offesa nei reati contro la libertà sessuale non contrasta con le disposizioni della Convenzione*, nota a C. eur. dir. uomo, sez. IV, dec. 30 agosto 2011, ric. n. 37334/08, G. c. Regno Unito, in *www.penalecontemporaneo.it* del 3 novembre 2011; CORBETTA S., *Le connotazioni strutturali dell'associazione con finalità di terrorismo anche internazionale*, in *Diritto penale e processo*, 2014, n. 2, p. 159 ss.; CORBETTA S., *Associazione con finalità di terrorismo internazionale: ammissibile il "concorso esterno"*, in *Diritto penale e processo*, 2007, n. 7, p. 580 ss.; SALVINI G., *L'associazione finalizzata al terrorismo: problemi di definizione e prova della finalità terroristica*, in *Cassazione penale*, 2006, n. 10, p. 3366 ss..

Corte di Cassazione penale, Sez. V, sentenza 11 novembre 2021, (ud. 15 luglio 2021), n. 41010/2021, Pres. Miccoli- Rel. Francolini

2. Ignoranza della minore età e siti d'incontri

L'avvenuta conoscenza su in sito di incontri riservato ai maggiorenni non può essere invocata a sostegno della circostanza che in buona fede l'autore di violenza sessuale abbia creduto che la sua interlocutrice avesse almeno 18 anni. In proposito la Corte ha confermato il giudizio di merito che aveva **escluso la ricorrenza in capo all'imputato d'ignoranza inevitabile dell'età della persona offesa** ai sensi dell'art. 609-sexies c.p., evidenziando come secondo orientamento unanime **essa ricorra solo quando non possa essere mosso neppure un rimprovero di semplice leggerezza**, essendo stato fatto tutto il possibile per adempiere ai doveri di attenzione, di conoscenza, di informazione e di controllo. **Uno sforzo di diligenza di questo tipo non può ritenersi assolto con l'"affidamento" ad un sito internet** ed alle regole che lo governerebbero, le quali non danno alcuna garanzia sulla veridicità dell'identità degli iscritti. Ad ulteriore conferma la Corte ha richiamato il fatto che **lo stesso ricorrente si era iscritto alla predetta piattaforma d'incontri come persona diversa**, indicando falsamente nome, età, aspetto fisico e professione, rendendosi, così, autore del reato di sostituzione di persona. Con riferimento a questo reato, è rappresentato, inoltre, come, essendo **il "vantaggio" che regge il dolo specifico identificabile con qualunque utilità o beneficio**, fosse costituito nel caso di specie dai contatti con giovanissime ragazze che il ricorrente cercava per la produzione di materiale pornografico e per avere rapporti sessuali.

Per approfondire: DELLI PRISCOLI L., *L'ignoranza dell'età del minore nei reati sessuali e le «nuove» sentenze interpretative, nota a Corte Costituzionale, sentenza 24/07/2007, n. 322*, in *Giurisprudenza costituzionale, 2008, n. 1*, p. 472 ss.; ARIOLLI G., *L'ignoranza dell'età della vittima nell'ambito dei delitti contro la libertà sessuale: un necessario contemperamento tra il principio di colpevolezza e le esigenze di tutela dell'intangibilità sessuale dei soggetti più deboli*, in *Cass. pen.*, 2008, p. 30 ss..; CORBETTA S., *Quando si realizza la violenza sessuale mediante sostituzione di persona*, in *Diritto penale e processo*, 2017, n. 1, p. 24 ss.; FORNASARI G., *Sostituzione di persona e amori clandestini*, in *Giurisprudenza italiana*, 2017, n. 2, p. 479 ss.; STAMPANONI BASSI G., *In tema di sostituzione di persona commessa nella rete*, in *Cassazione penale*, 2014, n. 1, p. 146 ss..; CRESCIOLI C., *Una sentenza della Cassazione sulla sostituzione di persona* online, in Dir. pen. cont., 21 giugno 2019.

Corte di Cassazione penale, sez. III, sentenza 17 novembre 2021, (udienza 28 settembre 2021), n. 41760/2021, Pres. Di Nicola-Rel. Mengoni

3. Concorso e assorbimento di reati informatici

Le condotte consistenti nell'**inserire apparecchiature skimmer nelle colonnine self- service di distributori di carburante** per intercettare i codici delle carte e riprodurli su carte clonate, successivamente utilizzate per il prelievo, sono punibili come **reati in concorso di frode informatica, ai sensi dell'art. 640 ter c.p., e d'indebito utilizzo di carte di credito e di pagamento, ai sensi dell'art. 493 ter c.p.** (formulazione antecedente alle modifiche introdotte con il d.lgs. n. 184/2021). Per la Corte la clonazione della carta ed il suo utilizzo sono **fatti autonomi, fisicamente distinti e successivi all'acquisizione dei codici con cui si consuma il reato di frode informatica**. E', invece, **assorbito dal delitto di frode il reato d'installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche**, il quale è configurabile ai sensi dell'art. 617-quinquies c.p. con riferimento all'installazione dello skimmer per intercettare la comunicazione al sistema informatico del pin della carta carburante. Per la Corte **se l'intercettazione avviene la condotta preparatoria d'installazione costituisce nei fatti uno dei modi di realizzazione dell'intervento illecito o dell'alterazione del funzionamento del sistema informatico** ai sensi dell'art. 640-ter c.p. e va, pertanto, punita esclusivamente come tale.

Per approfondire: GUERRA C., D'ANELLO P., *Il reato di frode informatica ed il rapporto con l'art. 55, comma 9, del D.Lgs. n. 231 del 2007. Dall' anamnesi agli elementi discretivi, alla luce del rapporto di specialità*, in *Diritto di Internet*, 2020, n. 4, p. 709 ss; CAPPITELLI R., *Ancora sulla distinzione tra indebito utilizzo di carte di pagamento e frode informatica*, in *Cassazione penale*, 2020, n. 10, p. 3828 ss.; ROSSI B., *Per l'integrazione del reato di cui all' art. 493-ter c.p. non occorre il conseguimento di un profitto o il verificarsi di un danno*, in *Cassazione penale*, 2019, n. 10, p. 3653 ss.; GALANTE A., *La tutela penale delle carte di pagamento*, in CADOPPI A., CANESTRARI S., MANNA A. e PAPA A. (a cura di),*Cybercrime*, Torino, 2019, p. 285 ss.; PICCINNI M., *Analisi di due tra i reati informatici più invasivi: l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche e l'installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche*, in *La Responsabilità amministrativa delle società e degli enti*, 2019, n. 1, p. 125 ss.; PICCARDI M., *In tema di abusiva installazione di apparecchiature atte ad intercettare comunicazioni telefoniche*, in *Cassazione penale*, 2009, n. 11, p. 4242 ss.

Corte di Cassazione penale, Sez. V, sentenza 18 novembre 2021, (ud. 07 settembre 2021), n. 42183/2021, Pres. Sabeone- Rel.Venegoni

4. Accesso abusivo e appropriazione indebita del dipendente

Lo "***ius excludendi alios***", garantito dall'art. 615-ter c.p. a tutela della privacy e della libertà del domicilio informatico, **si estende anche alle modalità che regolano l'accesso dei soggetti eventualmente abilitati o autorizzati** qualora mediante lo stesso sia stato ottenuto un risultato in contrasto con la volontà della persona offesa ed esorbitante l'eventuale ambito autorizzatorio. Per la Corte, inoltre, **integra sia il delitto di accesso abusivo, sia il delitto di appropriazione indebita**- a tutela del differente bene patrimonio - **la condotta del dipendente di una società, che incaricato di provvedere ai pagamenti dei fornitori in nome della stessa, si impossessi di somme di denaro sottraendole dal conto corrente aziendale**: l'accesso al sistema informatico, mediante utilizzo abusivo delle credenziali di autenticazione legittimamente detenute, consentendo la distrazione delle somme nel proprio esclusivo interesse, permette quella cd. *interversio possesionis* punibile ai sensi dell'art. 646 c.p..

Per approfondire: BARILE L., *Appropriazione indebita di file informatici: tra interpretazione estensiva e divieto di analogia. Il diritto penale è "cosa mobile"*, in *Sistema penale*, 2021, n. 3, p. 139 ss.; CIPOLLA P., *L'appropriazione indebita informatica nel contesto della dematerializzazione del concetto di cosa nei reati contro il patrimonio*, in *La Giustizia Penale*, 2020, n. 11, p. 605 ss.; SALVADORI I, *I reati contro la*

1

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 *Diritto penale e processo*, 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..

Corte di Cassazione penale, Sez. II, sentenza 07 dicembre 2021, (ud. 19 novembre 2021) n. 45196/2021, Pres. Diotallevi-Rel. Agostinacchio

5. L'irrilevanza della cancellazione di *file* pedoponografici e il requisito dell'"utilizzazione" del minore

La Corte di legittimità conferma **due consolidati orientamenti in materia di pornografia minorile**. Si tratta, in primo luogo, dell'orientamento secondo cui, **ai fini dell'integrazione del reato di cui all'art. 600-*quater* c.p., non ha alcuna rilevanza il mero trasferimento di *file* pedopornografici all'interno della cartella "cestino" del sistema operativo** di un computer in quanto gli stessi restano comunque disponibili mediante la semplice riattivazione dell'accesso al *file*. Nel caso di specie, benché la cancellazione delle foto da uno smartphone non preveda l'inserimento delle stesse in un cestino, è stato evidenziato che tanto il sistema Android che quello degli smartphone Apple consentono procedure piuttosto elementari e di comune conoscenza per ripristinare le immagini eliminate non in modo permanente: le immagini, recuperate e sequestrate, si trovavano in una cartella del cellulare denominata "eliminati di recente" e, quindi, erano di facile ed immediato ripristino.

In secondo luogo, si richiama l'orientamento, confermato dalle Sezioni Unite del 2018 (sentenza n. 51815 del 31/05/2018), secondo cui **risponde del delitto di pornografia minorile di cui all'art. 600-*ter* c.p., comma 1, n. 1, anche colui che, pur non realizzando materialmente la produzione di materiale pedopornografico, abbia istigato o indotto il minore a farlo** (come nel caso di specie, in cui sono state riscontrate modalità ingannevoli con le quali l'imputato induceva i minori alla realizzazione di materiale pornografico), facendo sorgere in questi il relativo proposito, prima assente, ovvero rafforzando l'intenzione già esistente, ma non ancora consolidata, in quanto tali condotte costituiscono una forma di manifestazione dell'utilizzazione del minore, che implica una strumentalizzazione del minore stesso, sebbene l'azione sia posta in essere solo da quest'ultimo e non assumendo valore esimente l'eventuale consenso prestato dallo stesso.

In senso conforme: Corte di Cassazione, sez. III penale, sentenza 8 marzo 2017 (ud. 07 aprile 2016), n. 11044/2017, Pres. Rosi - Rel. Gentili; Corte di Cassazione, sez. III penale, sentenza 14 gennaio 2019 (ud. 16 ottobre 2018) n. 1509/2019, Pres. Rosi - Rel. Scarcella; Corte di Cassazione, sez. III Penale, sentenza 19 marzo 2021 (ud. 11 febbraio 2021), n. 10759/2021, Pres. Ramacci - Rel. Corbetta.

Per approfondire: PICOTTI L., *La pedopornografia nel* Cyberspace: *un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale*, in *Diritto di Internet*, 2019, n. 1, p. 177 ss.; SALVADORI I., *Sexting, minori e diritto penale*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Torino, 2019, p. 567 ss.; ROSANI D., *Il trattamento penalistico del sexting in considerazione dei diritti fondamentali del minore d'età*, in *Rivista trimestrale di diritto penale contemporaneo*, 2019, n. 2, p 9 ss..

Corte di Cassazione, sez. III penale, sentenza 29 novembre 2021 (ud. 05 novembre 2021), n. 43615/2021, Pres. Gentili - Rel. Di Stasi.

6. Il pericolo di diffusione del materiale pedopornografico

Le Sezioni Unite n. 51815 del 31 maggio 2018 hanno ritenuto che ai fini dell'integrazione del reato di **produzione di materiale pedopornografico** di cui all'art. 600-*ter* co.1 c.p. n**on sia richiesto l'accertamento del concreto pericolo di diffusione di detto materiale**, superando l'interpretazione precedentemente fornita dalle stesse Sezioni Unite con la sentenza n. 13 del 2000. Tuttavia, questo cambio di orientamento, come confermato dalle stesse Sezioni Unite, n**on può essere qualificato come *overruling in malam partem***. Infatti,

l'art. 7 CEDU non consente l'applicazione retroattiva dell'interpretazione giurisprudenziale più sfavorevole di una norma penale solo quando il risultato interpretativo non era ragionevolmente prevedibile nel momento in cui la violazione è stata commessa. Tuttavia, in questo caso i**l mutamento giurisprudenziale era concretamente prevedibile dell'imputato**, poiché quando quest'ultimo ha registrato i due video pedopornografici col suo telefono cellulare nel 2016 **era già da tempo entrata in vigore la l. 6 febbraio 2006 n. 38**, che ha riformato l'art. 600-*ter* c.p. apportandovi rilevanti modifiche. Pertanto, l'imputato ben poteva rappresentarsi il fatto che non fosse più richiesto il concreto pericolo di diffusione di detto materiale.

In senso conforme: Corte di Cassazione, sez. un. penali, sentenza 15 novembre 2018 (ud. 31 maggio 2018), n. 51815/2018, Pres. Carcano – Rel. Andronio, con nota di PICOTTI L., *La pedopornografia nel* Cyberspace*: un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale riflessi nell'evoluzione normativa*, in *Diri. di Internet*, 2019, n. 1, p. 177 ss.

Per approfondire: SALVADORI I., Sexting, *minori e diritto penale*, in CADOPPI A., CANESTRARI S., MANNA A. e PAPA M. (a cura di), *Cybercrime*, Torino, 2019, p. 567 ss.; PICOTTI L., *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in BERTOLINO M., FORTI G. (a cura di), *Scritti per Federico Stella*, Napoli, 2007, vol. II, p. 1267 ss.;

Corte di Cassazione, sez. III penale, sentenza 17 dicembre 2021, (ud. 23 novembre 2021), n. 46184/2021, Pres. Di Nicola – Rel. Corbetta

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

NISCO A., *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*

Altre riviste e contributi

BORGIA G., *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, 11 novembre 2021.

CENTORAME F., *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. It. Dir. Pen. Proc.*, 2021, n. 2, p. 499 ss.

CRESCIOLI C., *Le diverse fasi dei* phishing attacks*: le fattispecie vigenti e i problemi applicativi in prospettiva comparata tra Italia e Germania*, in Ind. Pen., 2021, n. 3, p. 799 ss.

RUSSO A.C., *Captatore informatico e tutela dei diritti dell'individuo: tra presupposti applicativi e divieti probatori*, in *Dir. Pen. Proc*., 2021, n.11, p.

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