News maggio 2021

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

NOVITÀ SOVRANAZIONALI

1. Libertà di manifestazione del pensiero online

Il ricorrente lamentava la violazione dell'art. 10 della Convenzione europea dei diritti dell'uomo (CEDU) in quanto condannato da una Corte Regionale russa per aver reso disponibile sul proprio account *social* un contenuto video prodotto da terzi. Si trattava in particolare di un estratto di un noto film satirico, il quale tuttavia, estrapolato dal contesto in cui si inseriva e caricato privo di commenti o descrizioni, è stato qualificato dalle autorità competenti non quale forma di espressione satirica, ma quale incitamento pubblico ad atti di violenza a sfondo etnico-razziale.
Costituendo la condivisione di contenuti online una forma di manifestazione del pensiero, la Corte EDU ha riconosciuto la legittimità dell'interferenza realizzata dalle autorità pubbliche nell'esercizio di tale diritto, interferenza che deve, secondo quanto disposto dallo stesso art. 10 CEDU: essere prescritta dalla legge; perseguire uno o più scopi legittimi; essere necessaria in una società democratica per il raggiungimento di quegli stessi scopi.
Dopo aver evidenziato che il compito della Corte non è quello di sostituirsi alle competenti autorità nazionali, ma di valutare le decisioni adottate secondo il dettame degli articoli della CEDU, verificando che le stesse siano rette da ragioni rilevanti e sufficienti, la stessa ha rilevato che: il comportamento tenuto dal ricorrente è inquadrabile nell'ambito dell'art. 280 § 1 del codice penale russo, norma che punisce chi realizza pubblici incitamenti ad attività estremiste; la condanna può essere concepita quale volta alla prevenzione di forme di discriminazione razziale nonché alla tutela di diritti altrui (in questo caso diritto alla dignità) conformemente a quanto previsto dall'art. 10 CEDU; la condanna può ritenersi necessaria in una società democratica per il raggiungimento del suddetto fine in quanto forme di espressione che promuovono o giustificano violenza, odio, xenofobia o altre forme di intolleranza non possono rientrare nella tutela garantita dall'art. 10 CEDU, considerando anche che tali contenuti, se caricati su Internet, possono essere facilmente, grandemente e velocemente diffusi.
La Corte EDU, ritenendo non sussistente alcuna violazione dell'art. 10 CEDU nel caso di specie, ha sottolineato, infine, che il contenuto è stato pubblicato e diffuso su un gruppo online di un social media, al quale potevano accedere solamente gli "amici" a cui veniva concesso l'accesso dall'utente dell'account che ha caricato il materiale. La Corte EDU ha dunque riconosciuto l'effetto che tale atto ha nel rafforzare e radicalizzare le idee di un gruppo di persone "*like-minded*" senza che tali idee vengano esposte ad alcuna discussione critica o a visioni differenti.

Corte Europea dei Diritti dell'Uomo, 11 maggio 2021, app. n. 10271/12, Klin v. Russia

2. Intercettazioni di massa da parte delle autorità pubbliche e diritto al rispetto della vita privata

A seguito delle rivelazioni di Edward Snowden nel 2013, diverse associazioni non governative e giornalisti hanno proposto ricorso alla Corte EDU in quanto ritenevano che determinate operazioni di intercettazione di massa delle comunicazioni elettroniche svolte dal Regno Unito nell'ambito di attività d'*intelligence* per ragioni di sicurezza nazionale violassero gli artt. 8 e 10 CEDU. Si trattava in particolare di tre diversi regimi di sorveglianza: (1) l'intercettazione di massa delle comunicazioni; (2) la ricezione di materiale di intercettazione da governi stranieri e agenzie di *intelligence*; (3) l'ottenimento di dati di comunicazione dai fornitori di servizi di comunicazione.
La Corte ha ritenuto che, a causa della moltitudine di minacce che gli Stati devono affrontare nella società moderna, il funzionamento di un regime di intercettazione di massa non viola di per sé la Convenzione. Tuttavia, un tale regime deve essere soggetto a "garanzie *end-to-end*", il che significa che, a livello nazionale, dovrebbe essere fatta una valutazione della necessità e della proporzionalità delle misure adottate in ogni fase

del processo; che l'intercettazione di massa dovrebbe essere soggetta ad un'autorizzazione indipendente all'inizio, quando l'oggetto e la portata dell'operazione sono stati definiti; e che l'operazione dovrebbe essere soggetta alla supervisione e ad un esame indipendente *ex post*.
Per quanto riguarda il regime di intercettazioni di massa in vigore nel Regno Unito (disciplinato al tempo di realizzazione degli eventi di causa dal *Regulation of Investigatory Powers Act* del 2000, successivamente sostituito dall'*Investigatory Powers Act* del 2016), la Corte ha individuato una violazione dell'art. 8 CEDU in virtù delle seguenti carenze: le intercettazioni di massa sono state autorizzate dal Segretario di Stato, e non da un organismo indipendente dall'esecutivo; le categorie di termini di ricerca che definiscono i tipi di comunicazioni che potrebbero essere esaminate non sono state incluse nella richiesta di un mandato; e i termini di ricerca collegati a un individuo (vale a dire identificatori specifici come un indirizzo e-mail) non sono stati oggetto di una previa autorizzazione interna.
La Corte ha anche rilevato come il regime di intercettazione di massa violasse l'articolo 10, in quanto non prevedeva protezioni sufficienti per il materiale giornalistico riservato.
Anche il regime per l'ottenimento di dati sulle comunicazioni dai fornitori di servizi di comunicazione è stato ritenuto in violazione degli articoli 8 e 10, poiché non prevedeva alcun controllo da parte di un'autorità indipendente.
Tuttavia, la Corte ha ritenuto che il regime con il quale il Regno Unito poteva richiedere informazioni a governi stranieri e/o agenzie di *intelligence* era provvisto di sufficienti salvaguardie per proteggere i cittadini da eventuali abusi.

Corte Europea dei Diritti dell'Uomo, 25 maggio 2021, apps. n. 58170/13, 62322/14 and 24960/15, Big Brother watch and others v. The United Kingdom

3. Libertà d'espressione in relazione a compagne elettorali

Il ricorso presentato alla Corte EDU riguardava la censura della diffusione online di informazioni riguardanti elezioni politiche in un periodo pre-elezioni, ritenuta dai ricorrenti in violazione del proprio diritto di libera manifestazione del pensiero tutelato dall'art. 10 CEDU, mentre veniva qualificata dal governo russo quale misura legittima in quanto prevista da legge e necessaria in una società democratica al fine di garantire uno svolgimento delle elezioni politiche trasparente e privo di interferenze illecite.
In particolare, i ricorrenti (che non erano affiliati ad alcun partito politico, gruppo elettorale o candidato) affermavano che le informazioni pubblicate non potevano qualificarsi quale materiale di campagna elettorale e che dunque la loro pubblicazione non dovesse rispettare tutte le formalità previste dalla relativa normativa nazionale.
La Corte EDU, nel valutare la legittimità dell'interferenza rispetto al diritto di libera manifestazione del pensiero esercitata dalle autorità statali russe, ha evidenziato come la legge che costituiva fonte dell'interferenza stessa fosse diretta a regolare la divulgazione di informazioni relative alle elezioni realizzata solamente attraverso determinati *media*, quali la stampa, la radio e la televisione, mentre nulla risultava disposto in merito a compagne elettorali pre-elezioni realizzate attraverso Internet. Tale elemento non è stato considerato in ogni caso dirimente dal momento che la Corte EDU ha ritenuto applicabile al caso di specie le conclusioni raggiunte nel caso *Orlovskaya Iskra*, che riguardava la diffusione attraverso la stampa di informazioni relative alla campagna elettorale in periodo pre-elezioni, non ritenendo che la diversità del mezzo di comunicazione utilizzato pregiudicasse l'applicabilità delle stesse conclusioni.
Nel caso *Orlovskaya Iskra* la Corte concluse che il quadro normativo previsto dall'ordinamento russo riducesse eccessivamente e senza una giustificazione convincente lo spazio di espressione politica nella stampa, limitando la gamma dei partecipanti e delle prospettive. Tale quadro non ha dimostrato di raggiungere, in modo proporzionato, l'obiettivo di svolgere correttamente le elezioni. La Corte ha evidenziato come tale logica si applichi con ancora più forza nel contesto delle pubblicazioni online, che al giorno d'oggi tendono ad essere accessibili ad un maggior numero di persone e vengono considerate fonte importante di informazioni e idee.
Inoltre, la pubblicazione del contenuto sarebbe stata effettuata in un periodo precedente a quello relativo al c.d. silenzio elettorale che precede immediatamente le elezioni, risultandone dunque la limitazione non proporzionata agli interessi che si proponeva di tutelare. La Corte ha dunque accolto il ricorso riconoscendo sussistente la violazione dell'art. 10 CEDU.

In senso conforme: Corte Europea dei diritti dell'Uomo, 21 febbraio 2017, app. n. 42911/08, Orlovskaya Iskra v. Russia; Corte Europea dei diritti dell'Uomo, 25 febbraio 2020, app. n. 19273/08, Yartseva v. Russia.

Corte Europea dei diritti dell'Uomo, 18 maggio 2021 app. n. 43351/12, OOO Informatsionnoye Agentstvo Tambov-inform v. Russia

4. Parere del Garante europeo della protezione dei dati sulla strategia in materia di cybersicurezza

Il Garante europeo per la protezione dei dati personali, sostenendo e accogliendo con favore la proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, sottolinea alcuni punti che andranno a toccare la protezione dei dati personali nella gestione e garanzia di un livello adeguato di cybersicurezza, suggerendo alcune modifiche da apportare al testo della proposta. In particolare, il GEPD raccomanda di chiarire all'articolo 2 della proposta che la normativa dell'Unione in materia di protezione dei dati personali, in particolare il GDPR e la direttiva relativa alla vita privata e alle comunicazioni elettroniche, si applica a qualsiasi trattamento di dati personali che rientra nell'ambito di applicazione della proposta (invece che solo in contesti specifici); nonché di chiarire in un considerando che la proposta non mira ad incidere sull'applicazione delle norme vigenti dell'UE che disciplinano il trattamento dei dati personali, compresi i compiti e i poteri delle autorità di controllo indipendenti competenti a controllare il rispetto di tali atti. Inoltre, tra le altre, si evidenzia: la necessità di stabilire una definizione chiara e univoca del termine «cybersicurezza» ai fini della proposta; l'importanza dell'applicazione dei requisiti in materia di protezione dei dati fin dalla progettazione (*by design*) e per impostazione (*by default*) anche per la strategia in materia di cybersicurezza; ed infine, il ruolo fondamentale delle tecnologie di cifratura, determinanti e insostituibili per un'efficace protezione dei dati e della vita privata, la quale non dovrà dunque essere indebolita mediante soluzioni di «backdoor» o analoghe.

Sintesi del parere del Garante europeo della protezione dei dati sulla strategia in materia di cibersicurezza e sulla direttiva NIS 2.0

5. Consultazione EBA sull'istituzione di una banca dati centrale sull'antiriciclaggio e il contrasto al finanziamento del terrorismo

L'*European Banking Authority* (EBA) ha posto in pubblica consultazione, dal 6 maggio 2021 e fino al 17 giugno 2021, il progetto per l'istituzione di una banca dati centrale sull'antiriciclaggio e il contrasto al finanziamento del terrorismo.
La proposta posta in consultazione specifica sia il contenuto delle informazioni da raccogliere e il modo in cui dovranno essere comunicate, sia come saranno analizzate e potranno essere condivise a protezione e nel rispetto della riservatezza dei dati raccolti. In proposito l'EBA ha già richiesto il parere del Garante europeo della protezione dei dati (GEPD) e messo a disposizione dei partecipanti alla consultazione anche le specifiche tecniche relative al funzionamento della banca dati.
Le informazioni che dovranno essere trasmesse riguarderanno, in particolare, le carenze e criticità che le autorità competenti nazionali individueranno in relazione ai singoli istituti finanziari e le misure adottate per rettificarle.
Mediante questa banca dati si intende, così, creare uno strumento di "allarme preventivo": gli elementi raccolti saranno, infatti, analizzati e condivisi con le autorità nazionali e dell'Unione Europea per lo svolgimento delle rispettive attività di vigilanza, nonché potranno essere trasmessi, per gli approfondimenti necessari, alle Autorità Giudiziarie nazionali e all'EPPO (*European Public Prosecutor's Office*). In questo modo l'EBA potrà svolgere una più efficace azione di guida e coordinamento delle misure di prevenzione e contrasto al riciclaggio e al finanziamento del terrorismo.

Consultation on draft RTS on a central database on AML/CFT in the EU (EBA/CP/2021/19)

6. Consultazione ESMA sui rischi FinTech

La digitalizzazione sta trasformando la società, l'economia e il settore finanziario. L'applicazione di tecnologie innovative nel settore finanziario dell'Unione Europea può creare importanti benefici, riducendo le barriere geografiche e promuovendo una maggiore trasparenza, ma al contempo generando anche una serie di rischi relativi alla sicurezza informatica e alla gestione dei dati. La Commissione Europea mira ad affrontare questi rischi proponendo adeguamenti ai quadri legislativi esistenti entro la metà del 2022. L'*European Securities and Markets Authority* (ESMA) con la consultazione, che è stata avviata il 25 maggio 2021 e avrà termine il 1° agosto 2021, intende raccogliere le opinioni dei partecipanti al mercato al fine di supportare la Commissione nell'affrontare le future sfide regolamentari.

Call for evidence on digital finance

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Le nuove regole della Procura di Milano per le intercettazioni telematiche

Con la circolare interna del 24 maggio 2021 la Procura della Repubblica presso il Tribunale di Milano ha dettato alcune nuove regole per le società fornitrici di servizi a supporto delle intercettazioni telematiche, necessarie al fine di assicurare il tracciamento degli accessi e degli interventi realizzati sui *server* nonché la loro conservazione. In particolare, si richiede a tali società di utilizzare esclusivamente un captatore di loro proprietà, e non di società terze, del quale conoscano il funzionamento, di registrare le conversazioni soltanto sui *server* appositamente attestati, di utilizzare solo i *server* di c.d. "anonimizzazione od offuscamento" ubicati nel territorio nazionale e da utilizzare esclusivamente per il transito dei dati e non per la loro registrazione e, infine, di utilizzare applicazioni finalizzate all'inoculazione del virus visibili esclusivamente nello *store* della persona da intercettare.

Protocollo della Procura della Repubblica presso il Tribunale di Milano n.96331/21 E

2. Relazione del 13 maggio 2021 sullo stato dell'azione di prevenzione del riciclaggio e del finanziamento del terrorismo, per l'anno 2019, ai sensi dell'art. 4, comma 2, del decreto legislativo 21 novembre 2007, n. 231

Il 13 maggio 2021 il Comitato di Sicurezza finanziaria ha trasmesso la Relazione al Parlamento sullo stato dell'azione di prevenzione del riciclaggio e del finanziamento del terrorismo, dando atto della persistenza di vaste aree coperte dall'economia informale, nonché dall'uso del contante, con un connesso rischio di riciclaggio che è stato valutato molto significativo, mentre il rischio di finanziamento del terrorismo è stato valutato abbastanza significativo.
Nello specifico sulla base di 105.789 segnalazioni di operazioni sospette relative al 2019, di cui solo 770 relative al finanziamento del terrorismo, viene evidenziata, con riguardo al rischio di riciclaggio connesso a settori e strumenti innovativi, la centralità del ricorso ai *virtual asset* in connessione a truffe, frodi informatiche e abusivismo finanziario ed accanto a fenomeni di phishing, di ransomware, di distrazioni di fondi aziendali e di evasione fiscale spesso collegata a frodi nelle fatturazioni.
Il rischio relativo al finanziamento del terrorismo per azioni nel territorio nazionale rimane, invece, principalmente collegato ad un largo utilizzo del contante e ad importi modesti.
Quanto sopra dipende dal tipo di attività jihadiste rilevate in Italia e relativo per lo più alla diffusione di propaganda online ed all'apologia del terrorismo con conseguente capacità dei terroristi singoli o delle piccole cellule di autofinanziarsi facendo ricorso, anche, a fondi di origine lecita.
Per quanto riguarda, infine, il finanziamento del terrorismo internazionale, i casi emersi hanno documentato l'esistenza di reti di supporto finanziario in grado di trasferire in Siria le somme raccolte dai simpatizzanti

jihadisti in Europa principalmente attraverso l'*hawala* o altri sistemi bancari informali, nonché iniziative di *fund raising* avviate anche sulle piattaforme di messaggistica telematica.

Relazione sullo stato dell'azione di prevenzione del riciclaggio e del finanziamento del terrorismo per l'anno 2019

3. Dal Garante Privacy altre misure a tutela dei minori su TIK TOK

In data 12 maggio 2021, il Garante per la protezione dei dati personali, pur riconoscendo gli importanti risultati raggiunti a tutela dei minori, ha richiesto e ottenuto da Tik Tok l'impegno ad adottare ulteriori interventi al fine di tenere gli infratredicenni fuori dalla piattaforma. Tra queste misure appaiono particolarmente significative: la cancellazione, entro 48 ore, degli account segnalati e che risultino, all'esito di verifiche, intestati a utenti al di sotto dei 13 anni di età; l'elaborazione di soluzioni, anche basate sull'intelligenza artificiale, che consentano di minimizzare il rischio che bambini al di sotto dei 13 anni di età utilizzino la piattaforma; il rafforzamento di meccanismi di blocco dei dispositivi utilizzati dagli utenti infratredicenni per impedire l'accesso alla piattaforma; la condivisione con il Garante dei dati e delle informazioni relative all'efficacia delle diverse misure adottate.
Il Garante vigilerà sull'adempimento da parte di Tik Tok degli impegni assunti nell'ambito dei procedimenti ancora in corso nei confronti della piattaforma.

Da Tik Tok nuove misure per tenere i più giovani fuori dalla piattaforma. Intanto oltre 500mila gli account di infratredicenni già bloccati o rimossi

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Il rinvio pregiudiziale del Tribunale di Rieti in materia di acquisizione dei tabulati telefonici

Con ordinanza del 4 maggio 2021 il Tribunale di Rieti ha sollevato questione pregiudiziale innanzi alla Corte di Giustizia dell'Unione Europea affinché valuti la compatibilità dell'art. 132 co. 3 d.lgs. 30 giugno 2003 n. 196 (c.d. codice *privacy*) in tema di acquisibilità dei dati ottenibili dallo sviluppo di tabulati telefonici, con l'art. 15, par. 1, della Direttiva 2002/58/UE, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta di Nizza e dei principi stabiliti dalla Corte di Giustizia UE nella sentenza del 2 marzo 2021 nella causa C-746/18. In particolare, il Tribunale chiede alla Corte di Giustizia se il Pubblico ministero italiano possa essere considerato un organo terzo competente a disporre, mediante decreto motivato, l'acquisizione dei dati relativi al traffico e dei dati relativi all'ubicazione ai fini di un'istruttoria penale. Il Tribunale si preoccupa poi del fatto che un'eventuale applicazione retroattiva dei princìpi stabiliti nella sentenza del 2 marzo 2021 causa C-746/18, in assenza di una disciplina transitoria o di indicazioni intertemporali fornite dalla stessa CGUE, possa creare una paralisi delle indagini penali in corso e costituire un serio ostacolo all'accertamento e contrasto delle forme gravi di criminalità. Pertanto, come ulteriore questione pregiudiziale, il Tribunale domanda alla Corte di Giustizia UE se la normativa sovranazionale sopra menzionata possa essere interpretata nel senso di contemplare eccezionali ipotesi di "urgenza investigativa", tali da consentire al Pubblico Ministero l'immediata acquisizione dei dati dei tabulati telefonici, da ritenersi legittimamente acquisiti ove successivamente convalidati, in tempi rapidi, dal Giudice procedente.

In senso difforme: Corte di Cassazione, Sez. III penale, sentenza 2 dicembre 2019, (ud. 25 settembre 2019), n. 48737/2019, Pres. Lapalorcia – Rel. Reynaud; Corte di Cassazione, Sez. III penale, sentenza 23 agosto 2019 (ud. 19 aprile 2019), n. 36380/2019, Pres. Andreazza - Rel. Semeraro; Corte di Cassazione, sez. V penale, sentenza 19 luglio 2018, (ud. 24 aprile 2018), n. 33851/2018, Pres. Vessichelli – Rel. Morosini.

Per approfondire: LEO G., *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, in *Sist. Pen.*, 31

maggio 2021; TONDI V., *La disciplina italiana in materia di* data retention *a seguito della sentenza della Corte di giustizia Ue: il Tribunale di Milano nega il contrasto con il diritto sovranazionale*, in *Sist. Pen.*, 7 maggio 2021; MALACARNE A., *Ancora sulle ricadute interne della sentenza della Corte di Giustizia in materia di acquisizione di tabulati telefonici: il G.i.p. di Roma dichiara il "non luogo a provvedere" sulla richiesta del p.m.*, in *Sist. Pen.*, 5 maggio 2021; 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*, in *Sist. Pen.*, 29 aprile 2021; NERONI REZENDE I., *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, in *Sist. Pen.*, 2020, n. 5, p. 183 ss.; LUPARIA L., Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Dir. di Internet*, 2019, n. 4, p. 762 ss.; MARCOLINI S., *L'istituto della data retention dopo la sentenza della Corte di Giustizia del 2014*, in *Cybercrime* a cura di A. Cadoppi, S Canestrari, A. Manna, M. papa, Torino, 2019, p. 1579 ss.; CASTELLANI L., *Favoritismo ed abuso d'ufficio*, in *RGEA*, 2018, n. 2, pag. 51 ss.; FLOR R., Data retention e*d art. 132 Cod.* privacy: vexata quaestio (?), in *Dir. Pen. Cont.*, 29 marzo 2017; FLOR R., *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Riv. trim. Dir. Pen. Cont.*, 2014, n. 2, p. 178 ss; FLOR R., *Le recenti sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională *sul* data retention, in L. Violante, T. Galiani, A. Merli, *Oggetto e limiti del potere coercitivo dello Stato nelle democrazie costituzionali*, in *Annali della facoltà giuridica*, Camerino, 2013, p. 308 ss.; FLOR R., Data retention *e limiti al potere coercitivo dello Stato in materia penale: le sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională, in C*ass. pen.*, 2011, p. 1952 ss.; FLOR R., *Data retention rules under attack in the European Union? (Po sulmohen rregullat mbi ruajtjen e të dhënave në Bashkimin Evropian?)*, in *Illyrius*, 2012, p. 69 ss; FLOR R., *La tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională *su investigazioni ad alto contenuto tecnologico e* data retention, in L. Picotti, F. Ruggieri, *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, p. 32 ss.

Tribunale di Rieti, Sez. Penale, ordinanza del 4 maggio 2021, Pres. Sabatini – Rel. Marinelli

2. La Cassazione in merito al sequestro preventivo del sito *web*

La Suprema Corte, pronunciandosi in merito alla legittimità del sequestro preventivo del sito *web* del programma televisivo "Le Iene" ospitante dei servizi giornalistici sul virologo prof. Burioni, evidenzia che al sito *web* non può essere estesa la peculiare garanzia della non assoggettabilità a sequestro preventivo per il reato di diffamazione accordata alla stampa in senso tradizionale ed estesa dalla sentenza delle Sezioni Unite 17 luglio 2015, n. 31022, ric. Fazzo anche alla testata giornalistica telematica registrata. Infatti, con tale ultima pronuncia le Sezioni Unite non hanno fatto uso dello strumento dell'analogia, ma si sono limitate ad interpretare estensivamente il concetto di stampa. Pertanto, il semplice sito *web* non può godere della speciale garanzia sia perché non è prevista la sua registrazione presso il Tribunale, sia perché è privo di una figura che possa essere assimilata a quella del direttore responsabile di una testata giornalistica telematica registrata, chiamato giuridicamente a rispondere dei fatti diffamatori in forza di una specifica posizione di garanzia disciplinata dalla legge. Né può essere applicata al sito *web* la diversa disciplina di cui all'art. 30 della L. 6 agosto 1990, n. 223, dettata per le trasmissioni radiotelevisive e che non può certo essere applicata, sulla base di un'analogia in *malam partem*, alla pubblicazione *on line.*

Cft.: Corte di Cassazione, Sezioni Unite penali, sentenza 17 luglio 2015 (ud. 29 gennaio 2015), n. 31022/2015, Pres. Santacroce – Rel. Milo

Per approfondire: CORRIAS LUCENTE G., *Le testate telematiche registrate sono sottratte al sequestro preventivo. Qualche dubbio sulla "giurisprudenza legislativa"*, in *Dir. Inf. Inf.*, 2015, n. 6, pag. 1041 ss.; MELZI D'ERIL C., *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate on-line registrate*, in *Dir. Pen. Cont.*, 9 marzo 2016; VIMERCATI S., *La Cassazione conferma l'inestensibilità ai blog delle garanzie costituzionali previste per gli stampati in tema*

di sequestro, in *Dir. Pen. Cont.*, 26 ottobre 2016; CAMPANARO C., *Legittimo il sequestro preventivo del sito internet se i contenuti sono diffamatori*, in *Dir. Pen. Cont.*, 13 febbraio 2011.

Corte di Cassazione, sez. V Penale, sentenza 24 maggio 2021 (ud. 23 aprile 2021), n. 20645/2021, Pres. Sabeone – Rel. Tudino

3. Il reato di atti persecutori può essere commesso tramite *Facebook*

La Cassazione ribadisce che il delitto di atti persecutori di cui all'art. 612-*bis* c.p. ben può essere integrato dal reiterato invio alla persona offesa di messaggi su *Facebook*, in quanto a rilevare non è tanto il mezzo attraverso il quale si diffonde la comunicazione, ma piuttosto il contenuto della stessa, che deve costituire un comportamento concretamente vessatorio a danno della persona offesa. Peraltro, lo stesso legislatore, a seguito del d.l. 14 agosto 2013, n. 93, art. 1, comma 3, lett. a), convertito, con modificazioni, dalla L. 15 ottobre 2013, n. 119, ha introdotto al co. 2 dell'art. 612-*bis* c.p., la circostanza aggravante del fatto commesso "*attraverso strumenti informatici o telematici*", così chiarendo come tale delitto non solo può consumarsi anche attraverso tali modalità di comunicazione, ma in tal caso deve anche considerarsi connotato da un maggior disvalore sociale. Inoltre, evidenzia che quando il messaggio viene inviato al "profilo" della persona offesa, tale comunicazione non diverge da quelle veicolate con altro mezzo di diffusione poiché, in questo caso, si attua una diretta invasione della sfera privata altrui. Invece, quando il messaggio, pur rivolto ad una determinata persona, sia pubblicato sul profilo dell'imputato, va verificata la conoscibilità, che certamente sussiste qualora tale "profilo" sia ampiamente accessibile.

In senso conforme: Corte di Cassazione, Sez. VI penale, sentenza 30 agosto 2010 (ud. 16 luglio 2010), n. 32404/2010, Pres. De Roberto – Rel. Colla; Corte di Cassazione, Sez. V penale, sentenza 12 giugno 2019, (ud. 1 marzo 2019), n. 26049/2019, Pres. Palla – Rel. De Gregorio.

Corte di Cassazione, sez. V Penale, sentenza 31 marzo – 17 maggio 2021, n. 19363, Pres. Zaza – Rel. Scarlini

4. La detenzione di materiale pedopornografico e le circostanze aggravanti dell'ingente quantità e dell'uso di mezzi atti ad impedire l'identificazione

La Cassazione ribadisce che ai fini della sussistenza della circostanza aggravante della "ingente quantità" nel delitto di detenzione di materiale pedopornografico di cui all'art. 600-*quater* co. 2 c.p., si deve tener conto non solo del numero dei supporti informatici detenuti, ma anche del numero di immagini, da considerare come obiettiva unità di misura, che ciascuno di essi contiene. Pertanto, l'aggravante in esame risulta configurabile in ipotesi di detenzione di almeno un centinaio di immagini pedopornografiche, limite che rende in maggior misura percepibile il pericolo di implementazione del mercato illecito, che costituisce la ratio dell'inasprimento sanzionatorio. Inoltre, la Suprema Corte ribadisce che, sempre in tema di detenzione di materiale pedopornografico, l'aggravante dell'uso di mezzi atti ad impedire l'identificazione dei dati di accesso alle reti telematiche, di cui all'art. 602-ter co. 9 c.p., è configurabile nel caso in cui l'agente ponga in essere una qualunque azione volta ad impedire la sua identificazione, eludendo le normali modalità di riconoscimento, a partire da quelle relative all'accesso fisico al computer fino a quelle di inserimento nella rete stessa. Pertanto, ben può configurarsi l'aggravante in questione qualora l'imputato abbia scaricato le immagini pedopornografiche dal *web* mediante accesso ad apposito *link* con il sistema TOR, che consente di navigare sui siti pedopornografici senza far comparire il proprio indirizzo IP.

In senso conforme: Corte di Cassazione, sez. III penale, sentenza 16 novembre 2020 (ud. 8 ottobre 2020), n. 32166/2020, Pres. Di Nicola – Rel. Semeraro; Corte di Cassazione, Sez. III Penale, sentenza 30 agosto 2017 (ud. 27 giugno 2017), n. 39543/2017, Pres. Savani – Rel. Di Nicola; Corte di Cassazione, Sez. III Penale, sentenza 31 agosto 2016 (ud. 21 giugno 2016), n. 35876/2016, Pres. Rosi – Rel. Graziosi. (Sez. 3, n. 32166 del 08/10/2020, Rv. 280042 - 01)

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 7 aprile – 11 maggio 2021, n. 18153, Pres. Di Nicola – Rel. Di Stasi

5. La Corte costituzionale e il processo penale da remoto

La Corte Costituzionale ha dichiarato inammissibili le questioni di legittimità costituzionale sollevate con riferimento all'art. 3 del d.l. n. 28 del 2020, che ha ristretto l'ambito operativo delle udienze da remoto e delle relative camere di consiglio. Tale norma prevede che le disposizioni del processo da remoto non si applichino, salvo che le parti vi acconsentano, alle udienze di discussione finale, in pubblica udienza e a quelle nelle quali devono essere esaminati testimoni, parti, consulenti o periti. La Corte ha ritenuto che tale disposizione non sia affatto irragionevole, evidenziando che la disciplina succedutasi sul tema ha risentito, oltre che della necessità di trovare un ragionevole punto di sintesi tra il contenimento del contagio e la garanzia dei diritti della difesa, anche della esigenza di calibrare le diverse risposte normative, in particolare quella riguardante l'estensione dei presupposti per fare ricorso all'udienza penale da remoto sulla base dell'andamento della diffusione del contagio.

Corte Costituzionale, sentenza 11 maggio 2021 (ud. 15 aprile 2021), n. 96/2021, Pres. Coraggio – Rel. Petitti

6. Frode informatica e furto aggravato per violenza sulle cose

Il reato di frode informatica sussiste quando l'alterazione del sistema informatico è ciò che consente di ottenere il profitto. Nel caso in cui, invece, l'intervento sulla macchina è consistito nell'avere utilizzato indebitamente un codice per la apertura dei cassetti degli apparecchi, a cui è seguito un ordinario impossessamento fisico di quanto contenuto al loro interno, sarà configurabile il differente reato di furto eventualmente aggravato dal ricorso al mezzo fraudolento o alla violenza sulle cose, quali modalità che hanno reso possibile l'apprensione fisica del bene.

Per approfondire: PICOTTI L., *Reati Informatici*, in *Enc. Giur. Treccani*, Aggiornamento, VIII, Roma, 2000, p. 1 ss.; BARTOLI R., *La frode informatica tra "modellistica", diritto vivente e prospettive di riforma*, in *Dir. Inf.*, 2011, n. 3, p. 383 ss.; CAPPITELLI R., *La nozione di "mezzo fraudolento" nel delitto di furto aggravato tra implicazioni storiche e principio di offensività*, in *Cass. Pen.*, 2014, n. 5, p. 1651 ss.; TAMBURRO A., *Un'aggravante degli elastici confini: l'uso di mezzo fraudolento nel reato di furto*, in *Rivista penale*, 2014, n. 2, p. 131 ss.; MANICCIA A., *I recenti approdi della suprema Corte sui "liquidi" confini tra la truffa e il furto aggravato dal mezzo fraudolento*, in *Cass. Pen.*, 2018, n. 2, p. 561 ss.; SCORDAMAGLIA I., *Differenze tra il furto aggravato dall'uso del mezzo fraudolento e la truffa,* in *Dir. pen. e processo*, 2020, n. 3, p. 372 ss..

Corte di Cassazione, Sez. VI penale, sentenza del 17 maggio 2021 (ud. 2 marzo 2021), n. 19300/2021, Pres. Fidelbo - Rel. Di Stefano

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

L. GIORDANO, *La giurisprudenza di legittimità sulle prime applicazioni del processo penale telematico*, 21 maggio 2021

G. LEO, *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, 31 maggio 2021

L. TOMASI, *Diffamazione e illegittimità "convenzionale" della pena detentiva: oltre l'aggravante dell'uso della stampa?*, 3 maggio 2021

V. TONDI, *La disciplina italiana in materia di* data retention *a seguito della sentenza della Corte di giustizia Ue: il Tribunale di Milano nega il contrasto con il diritto sovranazionale*, 7 maggio 2021

Diritto di Internet, n. 3/2021

R. NIGRO, *Il Regolamento europeo sulla prevenzione della diffusione di contenuti terroristici online*

J. GOVERNA, *Jihad elettronica e partecipazione nel reato di organizzazione terroristica ex art. 270-bis c.p.*

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