News marzo 2021

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

NOVITÀ SOVRANAZIONALI

1. Trattamento di dati relativi a comunicazioni elettroniche e procedimento penale

Con la pronuncia sotto indicata, la Corte di Giustizia dichiara che l'articolo 15, paragrafo 1, della direttiva 2002/58 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, letto alla luce degli articoli 7, 8, 11 e 52 della Carta di Nizza, deve essere interpretato nel senso che esso osta alla normativa nazionale, che deve sempre conformarsi ai principi di equivalenza ed effettività, di consentire l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o all'ubicazione, idonei a fornire informazioni sulle comunicazioni elettroniche effettuate da un utente o sull'ubicazione delle apparecchiature utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo.

Lo stesso articolo impedisce inoltre che la normativa nazionale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di autorità pubbliche ai dati relativi al traffico e all'ubicazione ai fini di un'istruttoria penale, in quanto non in possesso dei necessari requisiti d'indipendenza che deve avere l'autorità incaricata di esercitare l'essenziale controllo preventivo sulla legittimità dell'accesso.

In senso conforme: Corte di Giustizia dell'Unione Europea, Grande Sezione, 6 ottobre 2020, C-511/18, C-512/18 e C-520/18.

Per approfondire: FLOR R., Data retention *e giustizia penale in Italia*, in PARODI C. (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, 2020, p. 683 ss.; ID., *Dalla* data retention *al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive* de jure condendo? In RESTA G., ZENO-ZENCOVICH V. (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015, p. 223 ss.

Corte di Giustizia dell'Unione Europea, Grande Sezione, 2 marzo 2021, C-746/2018

2. Tutela del diritto d'autore nel *cyberspace*

L'articolo 3, paragrafo 1, della direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, deve essere interpretato nel senso che costituisce una comunicazione al pubblico ai sensi di tale disposizione il fatto di incorporare, mediante la tecnica del framing, in una pagina Internet di un terzo, opere protette dal diritto d'autore, qualora tale incorporazione eluda misure di protezione contro il framing adottate o imposte dal titolare del diritto d'autore.
Al fine di garantire la certezza del diritto e il corretto funzionamento di Internet, le predette misure restrittive contro il framing devono essere, però, apposite ed efficaci, ai sensi dell'articolo 6, paragrafi 1 e 3, della direttiva 2001/29.
In presenza di queste misure di protezione ritenere che non costituisca una messa a disposizione ad un pubblico nuovo delle opere protette equivarrebbe a sancire una regola di esaurimento del diritto di comunicazione, privando il titolare del diritto d'autore della possibilità, di sfruttare commercialmente la messa in circolazione o la messa a disposizione dei materiali protetti. In questo modo sarebbe alterato il giusto equilibrio, che deve essere mantenuto, nell'ambiente digitale, tra la tutela degli interessi del titolare e quella della libertà di espressione e di informazione, garantita dall'articolo 11 della Carta, degli utilizzatori di questi materiali.

In senso conforme: Corte di Giustizia dell'Unione Europea, Grande Sezione, 7 agosto 2018, C-161/17.

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

Corte di Giustizia dell'Unione Europea, Grande Sezione, 9 marzo 2021, C- 392/19

3. La Dichiarazione n. 3/2021 dell'European Data Protection Board in merito alla proposta di Regolamento *e-privacy*

Con la Dichiarazione n. 3 adottata il 9 marzo 2021 l'European Data Protection Board ha fornito il suo parere in merito alla proposta del nuovo Regolamento *e-Privacy*. In particolare, l'EDPB esprime la sua preoccupazione per il fatto che tale nuovo Regolamento possa essere utilizzato per modificare *de facto* le disposizioni del Regolamento generale (c.d. GDPR). Con riferimento alla *data retention*, evidenzia che i nuovi artt. 6 co. 1 lett. d e 7 co. 4 non rispettano i canoni restrittivi dettati dalla giurisprudenza della Corte di Giustizia dell'Unione Europea in materia, poiché consentono una conservazione generale ed indiscriminata dei tabulati telematici sul traffico e sulla posizione del dispositivo dell'utente. L'EDPB sottolinea poi che le eccezioni introdotte dal nuovo art. 6 co. 1 lett. b, c, e d al divieto di trattamento sono troppo generiche e in tal modo consentono il pieno accesso da parte del fornitore di servizi di comunicazione elettronica o dei suoi responsabili ai contenuti di tutte le comunicazioni dell'utente, violando così il diritto alla riservatezza di quest'ultimo. A tal proposito, l'EDPB raccomanda l'uso di una crittografia forte e affidabile nel trattamento dei flussi elettronici in transito, a riposo o in lavorazione. Con riferimento ai c.d. *cookies*, l'EDPB evidenzia che il nuovo regolamento deve rispettare il principio del consenso, per cui la necessità di ottenere un autentico consenso liberamente prestato dovrebbe impedire ai fornitori di servizi di utilizzare pratiche sleali come soluzioni "prendere o lasciare" che subordinano l'accesso a servizi e funzionalità al consenso di un utente alla memorizzazione di informazioni od a concedere l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un utente (i c.d. *cookie walls*). Inoltre, la misurazione dell'*audience* dovrebbe essere limitata a pratiche non intrusive e non suscettibili di creare un rischio per gli utenti, mentre l'attuale modo per ottenere il consenso dovrebbe essere migliorato. Infine, con riferimento ai soggetti competenti per la vigilanza sull'applicazione del Regolamento *e-Privacy*, l'EDPB ribadisce che al fine di garantire parità di condizioni nel mercato unico digitale è essenziale garantire un'interpretazione e un'applicazione armonizzate di tutte le disposizioni sul trattamento dei dati in tutta l'UE. Pertanto, il controllo delle disposizioni in materia di *privacy* ai sensi del Regolamento *e-Privacy* dovrebbe essere affidato all'autorità competente di vigilanza come previsto dal Regolamento GDPR.

Dichiarazione n. 3 del 9 marzo 2021 dell'EDPB

4. Bussola per il digitale 2030: il modello europeo per il decennio digitale

Con questa comunicazione diffusa il 9 marzo 2021, facendo seguito alla strategia digitale del febbraio 2020 (consultabile al Topic *FinTech*), la Commissione europea ha delineato il programma per la politica digitale per il prossimo decennio. In particolare, al fine di conseguire la sovranità digitale in un mondo interconnesso, garantendo al contempo a cittadini e imprese un futuro digitale antropocentrico, nonché la sicurezza e la resilienza dell'ecosistema digitale, è prevista una struttura di *governance* condivisa con gli Stati membri basata su un sistema di monitoraggio annuale da sviluppare intorno ai seguenti quattro punti cardinali: 1) cittadini dotati di competenze digitali e professionisti altamente qualificati nel settore digitale; 2) infrastrutture digitali sostenibili, sicure e performanti; 3) trasformazione digitale delle imprese: entro il 2030 tre imprese su quattro dovrebbero utilizzare tecnologie digitali, tra cui il 5G, l'Internet delle cose, l'*edge computing*, l'intelligenza artificiale, la robotica e la realtà aumentata per sviluppare nuovi prodotti, nuovi processi di fabbricazione e nuovi modelli commerciali basati su un'equa condivisione dei dati nell'economia dei dati; 4) digitalizzazione dei servizi pubblici, compresi i sistemi giudiziari e, in particolare, le attività di indagine e di contrasto in modo da far fronte a reati digitali sempre più sofisticati.
Al fine di raggiungere questi obiettivi e specificatamente la sicurezza delle catene di approvvigionamento digitali, garantendo la governance di Internet con contrasto alla disinformazione e ai contenuti illeciti online,

nonché sostenere lo sviluppo della finanza digitale e dell'*e-government,* sono indicati anche progetti multinazionali e partenariati digitali internazionali.

La Commissione intende, inoltre,perseguire questi obiettivi ponendo le basi per una società digitale che sia informata al pieno rispetto dei diritti fondamentali dell'UE quali: la libertà di espressione, compreso l'accesso a informazioni diversificate, affidabili e trasparenti; la libertà di avviare e svolgere un'attività online; la protezione dei dati personali e della vita privata e il diritto all'oblio; la protezione della creazione intellettuale delle persone fisiche nello spazio online.
Fermi i principi relativi al mondo digitale fissati nel Trattato sull'Unione europea (TUE), nel Trattato sul funzionamento dell'Unione europea (TFUE), nella Carta dei diritti fondamentali e nella giurisprudenza della Corte di giustizia dell'Unione europea, è espressamente previsto che sia avviata una consultazione pubblica affinché possa essere sancito entro la fine del 2021 il quadro dei diritti e principi digitali in una dichiarazione interistituzionale solenne del Parlamento europeo, del Consiglio e della Commissione, analogamente al pilastro europeo dei diritti sociali.
In vista degli esiti della consultazione, nella Comunicazione sono, già, indicati come principi che dovranno orientare le decisioni politiche e le scelte degli operatori digitali: l'accesso universale a una connettività di alta qualità; la promozione di competenze digitali sufficienti affinché le persone possano partecipare attivamente alla società e ai processi democratici; lo sviluppo di servizi pubblici digitali ed accessibili; lo sviluppo di algoritmi antropocentrici e rispettosi di principi etici condivisi la promozione e garanzia di un ambiente online sicuro affinchè ciò che è illecito offline lo sia anche online; la responsabilizzazione e protezione dei minori nello spazio online.

Comunicazione Della Commissione Al Parlamento Europeo, Al Consiglio, Al Comitato Economico E Sociale Europeo E Al Comitato Delle Regioni (COM(2021) 118 final)

5. Autoveicoli connessi: le Linee Guida dell'European Data Protection Board

In data 9 marzo 2021 l'European Data Protection Board ha approvato le Linee Guida per i veicoli connessi e le applicazioni correlate alla mobilità. Con riferimento alle auto connesse, l'EDPB sostiene che l'industria automobilistica dovrebbe procedere nel rispetto dei principi di *privacy by design* e di *privacy by default*, in modo che gli apparati raccolgano e trasmettano la minor quantità possibile di dati riferibili alle persone presenti sul veicolo e solo per specifiche finalità. Il Garante sottolinea poi che per trattare i dati degli utenti di servizi quali assistenza alla guida, sicurezza stradale o servizi assicurativi, le aziende dovranno operare su una base giuridica, che per le auto connesse è fondata sul consenso degli interessati, ovvero guidatori e passeggeri, e sul principio di necessità. Inoltre, per servizi assicurativi di tipo *pay as you drive*, l'EDPB richiede che agli automobilisti sia fornita un'alternativa che non richieda l'installazione di *black box* e il tracciamento di mobilità. Nelle linee guida viene poi sostenuta l'importanza di fornire agli utenti informazioni comprensibili e nella loro lingua sul trattamento dei dati effettuato e di prevedere che conducenti e passeggeri possano attivare o disattivare autonomamente determinati servizi attraverso un'interfaccia di semplice utilizzo. L'EDPB raccomanda poi che quando possibile tutti i dati, in particolare quelli di geolocalizzazione, siano elaborati direttamente all'interno del veicolo e non trasmessi su un *cloud*, nonché di provvedere alla pseudonimizzazione o anonimizzazione dei dati o all'uso della crittografia, in modo da garantire l'integrità e la protezione dei dati. Particolare attenzione va poi posta con riferimento al trattamento dei dati biometrici.

Linee Guida EDPB n.1/2020 on processing personal data in the context of connected vehicles and mobility related applications adottate il 9 marzo 2021

6. Le Linee Guida dell'European Data Protection Board relative agli assistenti vocali virtuali

L'European Data Protection Board ha approvato in data 9 marzo 2021 le Linee Guida relative agli assistenti vocali digitali, oggi disponibili su *smartphone*, *tablet*, *computer* e altri *device*. Tali Linee Guida sono sottoposte a **consultazione pubblica** sino al 23 aprile 2021. In particolare, esse prevedono che gli *hardware* e *software* utilizzati siano automaticamente progettati per garantire maggiore trasparenza e riservatezza nell'uso dei dati, il cui trattamento costituisce una delle maggiori criticità con riferimento a tali sistemi. Inoltre, sottolineano che l'utente deve poter essere in grado di comprendere se il dispositivo è attivo o meno, oppure se lo stesso è in

ascolto o sta eseguendo un comando. L'EDPB sottolinea poi la necessità che la titolarità del trattamento dei dati sia definita con chiarezza e trasparenza, anche nel caso di fornitori di servizi specifici, in modo tale da garantire a tutti gli interessati la possibilità di esercitare efficacemente i propri diritti, come quello all'accesso, all'aggiornamento, alla cancellazione o alla portabilità dei dati. Inoltre, vi è la necessità di separare le finalità del trattamento dei dati, garantendo all'utente di poter esprimere liberamente il consenso per specifici trattamenti, quale *marketing*, profilazione o *machine learning* del servizio di intelligenza artificiale associato al dispositivo. L'EDPB raccomanda poi di provvedere alla pseudonimizzazione o anonimizzazione dei dati o all'uso della crittografia, in modo da garantire l'integrità e la protezione dei dati, in particolare di quelli biometrici, in modo che il riconoscimento della voce dell'utente avvenga sul dispositivo e non da remoto.

Linee Guida EDPB n. 2/2021 on Virtual Voice Assistants del 9 marzo 2021

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Relazione sulla politica dell'informazione per la sicurezza 2020

Come previsto dalla Legge 124/2007 sul Sistema di informazione per la sicurezza della Repubblica, è stata pubblicata il 1° marzo 2021 la "*Relazione sulla politica dell'informazione per la sicurezza*" per il 2020, curata dal Comparto Intelligence (DIS, AISE e AISI) e mediante la quale il Governo riferisce al Parlamento sulla politica dell'informazione per la sicurezza.
Tra i Focus trattati dalla relazione vi è la minaccia cibernetica, per cui viene delineato, in connessione all'emergenza pandemica, un significativo incremento. In particolare, gli attacchi censiti rilevano progettualità ostili (di matrice statuale, *hacktivista* o criminale), miranti a sfruttare il massiccio ricorso al lavoro agile in danno di operatori pubblici e privati, ovvero tese a carpire dati sensibili da strutture ospedaliere, centri di ricerca e realtà impegnate nello sviluppo di vaccini e terapie contro il Covid-19. I soggetti pubblici presi di mira sono stati soprattutto enti/operatori afferenti al settore della sanità e della ricerca e dicasteri ed altre Amministrazioni dello Stato, nei cui confronti si è registrata una intensa campagna di diffusione di malware e attacchi ransomware. Le azioni digitali ostili perpetrate nei confronti dei soggetti privati hanno, invece, interessato prevalentemente, oltre il settore farmaceutico/sanitario, quello bancario, i servizi IT e l'industria del Made in Italy. Sono state, in particolare, individuate attività di phishing, nonché la registrazione di domini malevoli allo scopo di ingannare gli utenti nel corso delle procedure di erogazione dei contributi economici per far fronte alla crisi economica generata dalla pandemia.
La Relazione dà, altresì, atto del contributo del Comparto Intelligence nella definizione della posizione nazionale in seno al Consiglio dell'Unione Europea con riguardo alle proposte di altri Stati Membri per l'emissione di misure restrittive nei confronti di soggetti e/o entità ritenuti responsabili di attacchi cyber, con effetti significativi, in danno di target europei, ai sensi del Regolamento del Consiglio Europeo 2019/796 e della Decisione del Consiglio 2019/797 del 17 maggio 2019. Le misure restrittive applicabili possono includere divieti di circolazione per le persone fisiche verso l'UE e congelamento di beni.
In coerenza con l'attribuzione al Comparto intelligence di nuove specifiche competenze in materia di cybersecurity, alla Relazione è, inoltre, allegato anche il Documento di Sicurezza Nazionale, concernente le attività relative alla protezione cibernetica e alla sicurezza informatica. In proposito sono evidenziati importanti avanzamenti nel processo di rafforzamento dell'architettura nazionale di sicurezza cibernetica, specie per quel che concerne: l'elaborazione dei decreti attuativi delle norme sul "Perimetro di sicurezza nazionale cibernetica"; l'implementazione della Direttiva europea NIS; la sicurezza delle reti 5G; le attività del Nucleo di Sicurezza Cibernetica e dello CSIRT (*Computer Security Incident Response Team*) italiano. Completano il novero delle iniziative intese a rafforzare la resilienza cyber del Paese quelle di carattere formativo e divulgativo, per una più diffusa consapevolezza e conoscenza di rischi e contromisure.

Relazione sulla politica dell'informazione per la sicurezza

2. Le disposizioni del Garante privacy per la tutela delle persone riprese in manette

Il Garante privacy ammonisce i *media* in merito alla diffusione e riproduzione di video e immagini che riprendono persone in manette. In particolare, evidenzia che al fine di non ledere la dignità delle persone e

garantire una tutela effettiva della loro immagine non è sufficiente *pixelare* le manette ai polsi di un fermato, se il soggetto ripreso risulta identificabile. Infatti, la sola *pixelatura* delle manette e dei polsi delle persone fermate, raffigurate in un contesto che rende palese la sussistenza di uno stato di costrizione fisica delle medesime, non è sufficiente a garantire la loro dignità. Inoltre, non contengono un'informazione essenziale. Pertanto, questo tipo di immagini violano il Codice privacy, nonché le regole deontologiche del giornalismo e del Codice di procedura penale.

Newsletter Garante Privacy n. 475 del 29 marzo 2021

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Ricevere *selfie* di minorenni nude da queste ultime realizzati non integra il reato di violenza sessuale

La realizzazione indotta di fotografie ritraenti le nudità di minori, senza il compimento ovvero la sopportazione di atti sessuali non integra il reato di violenza sessuale ex art. 609-*bis* c.p., dal momento che la nozione di "atti sessuali" implica necessariamente il coinvolgimento della corporeità sessuale del soggetto passivo, come nel caso della condotta di chi, per soddisfare o eccitare il proprio istinto sessuale, mediante comunicazioni telematiche che non comportino contatto fisico con la vittima, induca la stessa al compimento di atti che comunque ne coinvolgano la corporeità sessuale e siano idonei a violarne la libertà personale e non la mera tranquillità.
Per quanto riguarda la causa di non punibilità dell'ignoranza da parte del soggetto agente dell'età della persona offesa, che opera solamente qualora egli, pur avendo diligentemente proceduto ai dovuti accertamenti, sia indotto a ritenere sulla base di elementi univoci che il minorenne sia maggiorenne, non può ritenersi fondata nel caso di specie, in cui il ricorrente si è affidato solamente ai tratti fisici di sviluppo delle minorenni, tipici di maggiorenni, a rassicurazioni verbali circa l'età, nonché a considerazioni di natura generale relativamente allo scarso controllo genitoriale e alla già avvenuta pubblicazione di fotografie "spinte" in siti il cui accesso è consentito ai soli maggiorenni.

In senso conforme: Corte di Cassazione, sez. III penale, sentenza 11 ottobre 2019 (ud. 5 luglio 2019), n. 41951/2019, Pres. Andreazza - Rel. Scarcella; Corte di Cassazione, sez. III penale, sentenza 8 giugno 2011 (ud. 11 maggio 2011), n. 23094/2011, Pres. Teresi - Rel. Ramacci.

Per approfondire: PICOTTI L., *La violenza sessuale via whatsapp*, in *Diritto di Internet*, 2020, n. 4, p. 685 ss., in commento a Corte di Cassazione; sez. III Penale; sentenza 8 settembre 2020 (ud. 2 luglio 2020), n. 25266/2020, Pres. Rosi - Rel. Macrì.

Corte di Cassazione, sez. III penale, sentenza 26 marzo 2021 (ud. 6 novembre 2020), n. 11623/2021, Pres. Rosi - Rel. Cerroni

2. Diffusione di materiale pedopornografico e utilizzo di programmi di *file-sharing*

In tema di divulgazione e diffusione di materiale pedopornografico, la Corte richiama l'orientamento giurisprudenziale secondo cui è configurabile il dolo generico della condotta dell'utente che non si limiti alla ricerca e raccolta di immagini e filmati di pornografia minorile, tramite programmi di *file-sharing* o di condivisione automatica, ma operi una selezione del materiale scaricato, inserendo i prodotti multimediali in una apposita cartella di condivisione personalizzata.
L'elemento soggettivo del reato di cui all'art. 600-*ter* comma 3 c.p. non può dunque ritenersi provato dal solo utilizzo di un determinato tipo di programma di condivisione, quale Emule o simili, ma solo quando sussistano ulteriori elementi indicativi della volontà dell'agente di divulgare tale materiale, anche sotto il profilo del dolo eventuale, desumibili dall'esperienza dell'imputato, dalla durata del possesso del materiale, dalla sua entità numerica e dalla condotta connotata da accorgimenti volti a rendere difficoltosa l'individuazione dell'attività.
La Corte quindi afferma che chiunque, con adeguata esperienza informatica e con condotta non occasionale, utilizzi programmi di *file sharing* come Emule per scaricare dalla rete Internet materiale pedopornografico,

con la consapevolezza (derivante anche dalla circostanza che l'applicativo dia un apposito avviso a tale riguardo) che detto materiale, sino a quando non venga eliminato o spostato, resta in automatica condivisione con tutti gli altri utenti - essendo così oggettivamente diffuso in via telematica - laddove non provveda immediatamente a rimuovere il suddetto materiale dalla condivisione commette, quantomeno a titolo di dolo eventuale, il reato di pornografia minorile ex art. 600-*ter* comma 3 c.p..

In senso conforme: Corte di Cassazione, sez. III Penale, sentenza 26 marzo 2018 (ud. 14 dicembre 2017) n. 14001/2018, Pres. Di Nicola – Rel. Socci; Corte di Cassazione, sez. III penale, sentenza 8 maggio 2015 (ud. 13 gennaio 2015) n. 19174/2015, Pres. Fiale – Rel. Andronio.

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.; ID., *Commento Art. 600-ter, III comma, c. p. (Pornografia minorile)*, in CADOPPI A. (cur), *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, IV ed., Cedam, Padova 2006, p. 175 ss.

Corte di Cassazione, sez. III penale, sentenza 24 marzo 2021 (ud. 16 dicembre 2020), n. 11204/2021, Pres. Lapalorcia – Rel. Reynaud

3. Il concetto di "utilizzazione del minore" nel reato di produzione di materiale pedopornografico

Come affermato dalle Sezioni Unite (sentenza n. 51815 del 31/05/2018), il nuovo inquadramento sistematico della fattispecie punita dall'art. 600-*ter* comma 1 c.p., per effetto delle modifiche introdotte, da ultimo, con la L. n. 172 del 2012, "induce a valorizzare, allo scopo di evitare l'incriminazione di un comportamento evidentemente privo di rilevanza penale, il concetto cardine di 'utilizzazione del minore', enfatizzandone la portata dispregiativa, nel senso che esso implica una 'strumentalizzazione' del minore stesso".
Per "utilizzazione" deve dunque intendersi la trasformazione del minore, da soggetto dotato di libertà e dignità sessuali, in strumento per il soddisfacimento di desideri sessuali di altri o per il conseguimento di utilità di vario genere, condotta che rende invalido anche un eventuale consenso. Nel caso di specie, avendo l'imputato indotto una minore a compiere un rapporto orale nei suoi confronti e farsi fotografare e riprendere mediante un telefono durante tale atto, per poi divulgare tale materiale multimediale su diversi siti Internet, è stato ritenuto integrato il reato ex art. 600-*ter* comma 1 c.p. per aver l'imputato non solo carpito il video con l'inganno, ma anche minacciato la minore di divulgarlo.

In senso conforme: 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, 20 luglio 2018 (ud. 7 giugno 2018) n. 34162/2018, Pres. Savani - Rel. Galterio.

Corte di Cassazione, sez. III Penale, sentenza 19 marzo 2021 (ud. 11 febbraio 2021), n. 10759/2021, Pres. Ramacci - Rel. Corbetta

4. L'utilizzo di un falso profilo *social* integra i reati di sostituzione di persona e trattamento illecito dei dati personali

Con questa pronuncia la Suprema Corte ha ribadito che integra il delitto di sostituzione di persona la condotta di colui che crea ed utilizza un profilo su *social network* servendosi abusivamente della fotografia di un'altra persona inconsapevole, in quanto idonea alla rappresentazione di un'identità digitale non corrispondente al soggetto che ne fa uso. Inoltre, la descrizione poco lusinghiera che accompagna il profilo *social* evidenzia la sussistenza sia del fine di vantaggio, consistente nell'agevolazione delle comunicazioni e degli scambi di contenuti in rete, sia il fine di danno per il terzo, di cui è abusivamente utilizzata l'immagine e comporta che gli utilizzatori del servizio vengano tratti in inganno sulla disponibilità della persona associata all'immagine a ricevere comunicazioni a sfondo sessuale o sentimentale.
La Corte ha poi affermato che il reato di illecito trattamento dei dati personali, di cui all'art. 167 d.lgs. 30 giugno 2003 n. 196* ben può essere integrato dall'ostensione di dati personali del loro titolare ai frequentatori

di un *social network* attraverso l'inserimento degli stessi, previa creazione di un falso profilo, sul relativo sito, posto che il nocumento che ne deriva al titolare medesimo s'identifica in un qualsiasi pregiudizio giuridicamente rilevante di natura patrimoniale o non patrimoniale subito dal soggetto cui si riferiscono i dati protetti oppure da terzi quale conseguenza dell'illecito trattamento.

In senso conforme: Corte di Cassazione, sez. V penale, sentenza 23 luglio 2020 (ud. 6 luglio 2020) n. 22049/2020, Pres. Palla – Rel. Riccardi; Corte di Cassazione., sez. V penale, sentenza 19 luglio 2018 (ud. 18 giugno 2018), n. 33862/2018, Pres. Sabeone - Rel. Tudino; Corte di Cassazione, sez. V penale, sentenza 16 giugno 2016 (ud. 23 aprile 2014), n. 25774/2014, Pres. Dubolino – Rel. Lignola; Corte di Cassazione, sez. V penale, sentenza 29 aprile 2013 (ud. 28 novembre 2012) n. 18826/2013, Pres. Zecca – Rel. Guardiano; Corte di Cassazione, sez. III penale, sentenza 17 ottobre 2019 (ud. 28 maggio2019) n. 42565/2019, Pres. Izzo – Rel. Ramacci; Corte di Cassazione, sez. III penale, sentenza 20 novembre 2018 (ud. 19 giugno 2018) n. 52135/2018

Per approfondire: CRESCIOLI C., *Profili penali della creazione di un falso profilo Facebook a scopo diffamatorio*, in *Dir. di Internet*, 2020, n. 4, p. 701 ss.; MARRAFFINO M., *La sostituzione di persona mediante furto di identità digitale*, in *Cybercrime* a cura di Cadoppi, Canestrari, Manna e Papa, Torino, 2019, p. 307 ss.; CRESCIOLI C., *Una sentenza della Cassazione sulla sostituzione di persona* online, in *Dir. pen. cont.*, 21 giugno 2019; SANSOBRINO F., *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in *Dir. pen. cont.*, 30 settembre 2014; GIUDICI A., *Creazione di un falso profilo utente sulla rete e delitto di sostituzione di persona*, in *Dir. pen. cont.*, 25 giugno 2013; PICOTTI L., *I diritti fondamentali nell'uso ed abuso dei social network. aspetti penali*, in *Giur. Mer.*, 2012, n. 12, p. 2522 ss.; FLICK C., *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, in *Dir. inf. inf.*, 2008, p. 526 ss.; PICOTTI L., *Profili penali delle comunicazioni illecite via Internet*, in *Dir. inf. inf.*, 1999, p. 283 ss.

* La Suprema Corte non specifica il riferimento è all'art. 167 d.lgs. 30 giugno 2003 n. 196 nella sua originaria forumlazione o in quella modificata dal d.lgs 10 agosto 2018 n. 101. Nel novellato art. 167 cit., infatti, tra le condotte sanzionate è stata eliminata la violazione dell'abrogato art. 23 d.lgs.196/2003, ovvero il trattamento di dati personali avvenuto senza consenso dell'interessato, mentre vengono punite soltanto la violazione delle disposizioni di cui agli artt. 123 (dati relativi al traffico), 126 (dati relativi all'ubicazione), 130 (comunicazioni indesiderate) e 129 (dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico) del d.lgs. 196/2003. Il co. 2 della versione attuale dell'art. 167 cit., invece, individua come dati personali penalmente tutelati solmente categorie particolari di dati personali, nonché i dati personali relativi a condanne penali e reati.

Corte di Cassazione, sez. V Penale, sentenza 5 febbraio – 30 marzo 2021, n. 12062, Pres. Pezzullo – Rel. Scordamaglia

5. Pubblicazione sui *social network* di materiale inneggiante all'Isis e apologia di terrorismo

Con questa sentenza la Corte di Cassazione ribadisce che i reati di istigazione a delinquere e di apologia di delitto, puniti dai co. 1 e 3 dell'art. 414 c.p., costituiscono fattispecie di pericolo concreto e richiedono perciò per la loro configurazione un comportamento che sia concretamente idoneo, sulla base di un giudizio *ex ante*, a provocare la commissione di delitti. Pertanto, è idonea a integrare il reato di apologia di delitti di terrorismo la condotta di chi condivida su *social network* dei *link* a materiale *jihadista* di propaganda, anche senza pubblicarli in via autonoma, in quanto, potenziando la diffusione di detto materiale, tale condotta accresce il pericolo non solo di emulazione di atti di violenza ma anche di adesione, in forme aperte e fluide, all'associazione terroristica che li propugna, dato che il pericolo concreto può concernere anche l'adesione di taluno a un'associazione terroristica ex art. 270 bis c.p. A tal proposito, non ha nessun rilievo che il numero di *follower* del profilo *social* e di *like* e condivisioni apposti ai *file* condivisi o postati sia ridotto, poiché, stante la pacifica natura di reato di pericolo dell'art. 414 c.p., per integrare il reato è sufficiente la concreta possibilità che la diffusione di documenti di contenuto apologetico e propagandista inneggianti allo Stato islamico e alle attività terroristiche dell'Isis crei o comunque incrementi il rischio potenziale di commissione di reati lesivi di beni omologhi rispetto a quelli offesi dai crimini esaltati.

In senso conforme: Corte di Cassazione, sez. V penale, sentenza 27 novembre 2019 (ud. 12 settembre 2019), n. 48247/2019, Pres. Vessichelli – Rel. Caputo; Corte di Cassazione, sez. I penale, sentenza 15 novembre 2018 (ud. 9 ottobre 2018), n. 51654/2018, Pres. Rocchi – Rel. Santalucia; Corte di Cassazione, sez. I penale, sentenza 1 dicembre 2015 (ud. 6 ottobre 2015), n. 47489/2015, Pres. Chieffi – Rel. Rocchi; Corte di Cassazione, sez. V penale, sentenza 16 gennaio 2019, (ud. 26 settembre 2018), n. 1970, Pres. Zaza – Rel. Riccardi

Per approfondire: PICOTTI L., *Terrorismo e sistema penale: realtà, prospettive, limiti*, in *Dir. Pen. Cont. Riv. Trim.*, 2017, n. 1, p. 249 ss.; ZIRULIA S., *Apologia dell'IS via internet e arresti domiciliari. Prime prove di tenuta del sistema penale rispetto alla nuova minaccia terroristica*, in *Dir. pen. cont.*, 14 dicembre 2015; DAMBRUOSO S., *Il cyberterrorismo di matrice religiosa*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA A. (a cura di), *Cybercrime*, Torino, 2019, p. 217 ss.; FLOR R., *Perspective for new types of "technological investigation" and protection of fundamental rights in the Era of Internet. The so-called "cyberterrorism" as a prime example, between problems of definition and the fight against terrorism and cybercrime*, in *Delito, pena, politica criminal y tecnologìas de la informatiòn en las modernas ciencias penales*, Salamanca, Ediciones Universidad de Salamanca, 2012, p. 51 ss.; SIEBER U., BRUNST P., *Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions*, in *Council of Europe* (ed.), *Cyberterrorism – the use of the Internet for terrorist purposes*, Strasbourg, Council of Europe Publishing, 2007

Corte di Cassazione, sez. I penale, sentenza 25 marzo 2021 (ud. 27 gennaio 2021), n. 11581/2021, Pres. Tardio - Rel. Sandrini

6. Diffamazione su *Facebook* di operai al lavoro

Integra il reato di diffamazione la pubblicazione sul proprio profilo Facebook di una fotografia che riprendeva quattro operai del Comune di Cecina durante lo svolgimento delle loro mansioni, con la seguente didascalia: "*stazione di Cecina, uno lavora, uno tiene il secchio e due si occupano di relazioni istituzionali, una specie di corpo diplomatico*".
Per la Corte non è fondata quella critica che sulla base di un singolo momento dell'attività lavorativa ne investa l'intera portata o, meglio, la diligenza e l'impegno di coloro che vi sono coinvolti e di cui viene offesa la reputazione: si tratta di una rappresentazione suggestiva nella misura in cui lascia intendere ai destinatari della comunicazione che quel singolo episodio sia espressione di una condotta generalizzata.

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., 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.

Corte di Cassazione, sez. V Penale, sentenza 24 marzo 2021 (ud. 4 marzo 2021), n. 11426/2021, Pres. Palla - Rel. De Marzo

7. La Cassazione e la compatibilità del captatore informatico coi principi costituzionali

La Suprema Corte ribadisce il principio di diritto affermato dalle Sezioni Unite nel ricorso Scurato (sentenza dep. 1 luglio 2016 (ud. 28 aprile 2016), n. 26889/2016, Pres. Giovanni Canzio – Rel. Vincenzo Romis) secondo cui per l'attività di intercettazione tramite *trojan horse*, realizzata prima dell'entrata in vigore della specifica disciplina legislativa, trova applicazione la disciplina delle intercettazioni tra presenti di cui agli artt. 266, 267 e 271 c.p.p., con le peculiarità introdotte per i reati di criminalità organizzata dal d.l. n. 152 del 1991, art. 13, convertito dalla l. n. 252 del 1991. Pertanto, secondo la normativa previgente, il captatore informatico ben poteva essere utilizzato per realizzare intercettazioni tra presenti nei procedimenti per delitti di criminalità organizzata. Le Sezioni Unite hanno poi precisato che il cd. *trojan horse* permette la captazione anche nei luoghi di privata dimora, prescindendo dall'indicazione di questi come sede di attività criminosa in atto, per

cui la preventiva individuazione di tali luoghi non era affatto necessaria. Dev'essere, dunque, ritenuta legittima l'intercettazione tra presenti eseguita a mezzo di captatore informatico nell'ambito di attività investigativa svolta in relazione a procedimenti per delitti di criminalità organizzata, senza che sia necessaria la preventiva individuazione ed indicazione dei luoghi in cui la captazione deve essere espletata.
La Suprema Corte osserva poi che le Sezioni Unite hanno già valutato la compatibilità dell'utilizzo del captatore informatico nelle indagini per i delitti di criminalità organizzata con i principi costituzionali, tenendo conto dell'eccezionale gravità e pericolosità di tali reati per l'intera collettività. Inoltre, evidenzia che il bilanciamento tra il soddisfacimento dell'interesse pubblico all'accertamento di gravi delitti con il principio di inviolabilità della sfera di riservatezza e segretezza di qualsiasi forma di comunicazione opera anche in relazione al diritto di proprietà privata di cui all'art. 42 Cost., avuto riguardo all'utilizzazione, mediante l'intercettazione con virus trojan, dell'energia acquistata dall'indagato per la ricarica delle batterie del dispositivo elettronico "infettato" ed all'utilizzo di quest'ultimo. Infatti, le conseguenze di perdita di una quota del proprio diritto di proprietà da parte del soggetto intercettato, peraltro non particolarmente consistente dal punto di vista patrimoniale, appaiono recessive, rispetto all'obiettivo, egualmente legittimo, del soddisfacimento dell'interesse pubblico all'accertamento di gravi delitti, tutelato dal principio, di pari rango costituzionale, dell'obbligatorietà dell'azione penale di cui all'art. 112 Cost.

In senso conforme: Corte di Cassazione, sez. V penale, sentenza 11 novembre 2020 (ud. 30 settembre 2020), n. 31604/2020, Pres. Vessichelli – Rel. Morosini; Corte di Cassazione, Sez. Unite penali, sentenza 1 luglio 2016 (ud. 28 aprile 2016), n. 26889/2016, Pres. Canzio – Rel. Romis, con nota di PICOTTI L., *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. Pen.*, 2016, n. 2, p. 1 ss. e CAJANI F., *Odissea del captatore informatico*, in *Cass. Pen.*, 2016, n. 11, p. 4140 ss.; Corte di Cassazione, Sez. Unite Civili, sentenza 15 gennaio 2020 (ud. 3 dicembre 2019), n. 741/2020, Pres. Curzio – Rel. Sambito

Per approfondire: TORRE M., *Le intercettazioni a mezzo del c.d. captatore informatico o "trojan di Stato"*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Torino, 2019, p. 1660 ss.; TROGU M., *La disciplina intertemporale sull'uso del captatore informatico ai fini dell'intercettazione di comunicazioni tra presenti*, in *Proc. pen. giust.*, 2020, n. 5, p. 1243 ss.; BENE T., "*Il re è nudo": anomie disapplicative a proposito del captatore informatico*, in *Arch. pen. web*, 2019, n. 3; BONTEMPELLI M., *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont.*, 20 dicembre 2018; CALAVITA O., *L'odissea del trojan horse*, in *Dir. pen. cont.*, 2018, n. 11, p. 45 ss.; GIORDANO L., *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in SP, 2020, n. 4, p. 109 ss.; PITTIRUTI M., *L'apprensione all'estero della prova digitale*, in LUPÁRIA L., MARAFIORI L., PAOLOZZI G. (a cura di), *Dimensione tecnologica e prova penale*, Torino, 2019, p. 205 ss.; LORENZETTO E., *Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico"*, in *Dir. pen. cont.*, 24 marzo 2016; LUPÁRIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica*, Milano, 2007;

Corte di Cassazione, sez. V penale, sentenza 22 marzo 2021 (ud. 30 settembre 2020), n. 10981, Pres. Vessichelli - Rel. Calaselice

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

BARILE L., *Appropriazione indebita di file informatici: tra interpretazione estensiva e divieto di analogia il diritto penale è "cosa mobile"*

DI DOMENICO A., *La Cassazione sulle intercettazioni mediante trojan disposte dal pubblico ministero: la convalida preclude ogni discussione sul requisito dell'urgenza*

RINCEANU J., *Verso una forma di polizia privata nello spazio digitale? L'inedito ruolo dei* provider *nella disciplina tedesca dei* social network

PAGELLA C., *La Cassazione sulla riconducibilità dei file al concetto di "cosa mobile" oggetto di appropriazione indebita: un caso di analogia* in malam partem*?*

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