News settembre-ottobre 2021

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

NOVITÀ SOVRANAZIONALI

1. Limiti alla libertà d'espressione in Facebook

Il caso oggetto della pronuncia sotto indicata riguardava la condanna penale del ricorrente, all'epoca consigliere comunale candidato alle elezioni del Parlamento francese, per incitamento all'odio o alla violenza contro un gruppo di persone o un individuo a causa della loro appartenenza a una specifica religione. Il ricorrente era stato ritenuto responsabile dalle autorità francesi a seguito della sua mancata azione tempestiva nella cancellazione di commenti pubblicati da altri sulla bacheca del suo account Facebook. Il tribunale francese aveva infatti concluso che, avendo il ricorrente creato di sua iniziativa un servizio di comunicazione pubblica per via elettronica allo scopo di scambiare opinioni, e avendo lasciato i commenti incriminati visibili, il signor Sanchez non aveva agito tempestivamente per fermarne la diffusione ed era quindi colpevole come "produttore" di un sito di comunicazione pubblica online, e quindi come autore del reato.
La Corte ha ribadito che la tolleranza e il rispetto della pari dignità di tutti gli esseri umani costituiscono le basi di una società democratica e pluralista. Di conseguenza, si potrebbe in linea di principio considerare necessario punire o addirittura impedire tutte le forme di espressione che diffondono, incitano, promuovono o giustificano l'odio basato sull'intolleranza.
La Corte ha sottolineato come siano necessarie ragioni molto forti per giustificare le restrizioni al discorso politico e che nel periodo che precede le elezioni, le opinioni e le informazioni di ogni tipo dovrebbero poter circolare liberamente. Nelle circostanze specifiche del caso, tuttavia, la Corte ha rilevato che la decisione dei giudici nazionali di condannare il ricorrente per non aver agito tempestivamente nel cancellare i commenti chiaramente illegali pubblicati da altri sulla bacheca del suo account Facebook, utilizzato nell'ambito della sua campagna elettorale, era basata su motivi pertinenti e sufficienti legati alla mancata vigilanza e reattività.
La Corte ha osservato che il ricorrente non era stato criticato per aver fatto uso del suo diritto alla libertà di espressione, in particolare nel contesto del dibattito politico, ma era stato accusato di una mancanza di vigilanza e di reattività in relazione ai commenti pubblicati sulla bacheca del suo account Facebook. La Corte ha quindi concluso che sia il Tribunale penale che la Corte d'appello hanno basato il loro ragionamento sulla responsabilità del ricorrente su motivi pertinenti e sufficienti ai fini dell'art. 10 della Convenzione. I giudici nazionali avevano infatti stabilito la responsabilità del ricorrente sulla base di diversi fattori. Egli aveva consapevolmente reso pubblica la bacheca del suo account Facebook, consentendo così ai suoi amici di pubblicarvi commenti. Aveva quindi il dovere di controllare il contenuto delle dichiarazioni pubblicate. Inoltre, il tribunale penale aveva sottolineato che il ricorrente non poteva ignorare che il suo account fosse suscettibile di attirare commenti di natura politica e polemici, che quindi avrebbero dovuto essere controllati ancora più attentamente. La Corte d'appello aveva ritenuto, in modo simile, che il suo status di personaggio politico richiedeva una vigilanza ancora maggiore da parte sua.
La Corte EDU ha quindi ritenuto "necessaria in una società democratica" l'interferenza delle autorità francesi al diritto alla libertà d'espressione del ricorrente escludendo la violazione dell'art. 10 (libertà di espressione).

Corte Europea dei diritti dell'uomo, 2 settembre 2021, app. n. 45581/15, Sanchez v. France

2. *Cyberstalking* e violazione dell'art. 8 della Carta Europea dei diritti dell'Uomo

Nel caso Volodina v. Russia, la Corte europea dei diritti dell'uomo ha dichiarato, all'unanimità, la sussistenza di una violazione dell'art. 8 (diritto al rispetto della vita privata) della Convenzione europea dei diritti dell'uomo. La ricorrente si era rivolta alla Corte EDU sostenendo che le autorità russe non erano riuscite a proteggerla dalle ripetute condotte di *cyber*-violenza poste in essere dal suo compagno, il quale aveva creato

profili falsi a suo nome, pubblicato sue foto intime, seguito i suoi movimenti e inviato minacce di morte tramite i *social media*.
La Corte ha rilevato che, pur avendo a disposizione gli strumenti legali (sia di diritto civile che di diritto penale) per perseguire il partner della ricorrente, le autorità non hanno svolto un'indagine efficace e non hanno considerato in nessun momento ciò che avrebbe potuto e dovuto essere fatto per proteggere la ricorrente dalle persistenti molestie online. Dopo che erano state raccolte prove sufficienti per accusare il colpevole, le indagini non sono andate oltre lo stadio del sospetto, e la risposta delle autorità russe al rischio noto di violenze ricorrenti è stata quindi manifestamente inadeguata e, attraverso la loro inerzia e mancata adozione di misure deterrenti, hanno permesso al colpevole di continuare a minacciare, molestare e aggredire la ricorrente. Le autorità sono quindi venute meno ai loro obblighi di proteggere la vittima da gravi abusi ai sensi dell'art. 8 CEDU.
Queste conclusioni rispecchiano quelle di una precedente sentenza riguardante la stessa ricorrente, Volodina v. Russia (n. 41261/17), in cui la Corte europea ha sempre ritenuto la risposta delle autorità russe ai ripetuti atti di violenza domestica quale manifestamente inadeguata.

Corte Europea dei diritti dell'uomo, 14 settembre 2021, app. n. 40419/19, Volodina v. Russia

3. Intelligenza artificiale e machine learning: la guida IOSCO

A settembre 2021, all'esito della consultazione pubblica, l'Organizzazione internazionale delle Autorità di controllo dei mercati finanziari (IOSCO) ha diramato la guida relativa alla supervisione di intermediari e gestori patrimoniali che usano sistemi di intelligenza artificiale (AI) e machine learning (ML).
Le misure proposte sono suddivise nelle seguenti sei aree d'intervento: 1. la creazione di una conforme governance con chiari profili di responsabilità per lo sviluppo, l'implementazione e il monitoraggio di AI e ML; 2. la realizzazione di test idonei a verificare come gli algoritmi operino in condizioni peculiari e se siano effettivamente rispettosi della normativa di riferimento prima della loro piena implementazione; 3. lo sviluppo di competenze tecniche da parte delle funzioni di compliance interessate; 4. la definizione di accordi chiari e precisi, soprattutto in termini di riparto di responsabilità, con i fornitori dei sistemi di IA e ML; 5. la previsione, nei servizi erogati di IA e ML, di obblighi informativi a favore delle autorità di controllo e dei clienti sul loro impiego; 6. l'imposizione di controlli periodici in funzione di prevenzione ed emersione di possibili gap o distorsioni sui sistemi di IA e ML implementati.

The use of artificial intelligence and machine learning by market intermediaries and asset managers

4. Proposta Commissione Europea per la trasformazione digitale entro il 2030

In data 15 settembre 2021 la Commissione Europea ha presentato la proposta di_un piano concreto per conseguire la trasformazione digitale della società e dell'economia dell'UE entro il 2030. Lo scopo del piano è istituire un quadro di governance basato su un meccanismo di cooperazione annuale con gli Stati membri e volto a conseguire gli obiettivi del decennio digitale per il 2030 a livello dell'Unione nei settori delle competenze digitali, delle infrastrutture digitali e della digitalizzazione delle imprese e dei servizi pubblici. All'art. 2 del proposto piano la Commissione ha, in particolare, ribadito che tra gli obiettivi da raggiungere congiuntamente con gli Stati vi sono la promozione di un ambiente digitale antropocentrico aperto, connotato da tecnologie e servizi digitali conformi ai principi ed ai valori dell'Unione, ed il rafforzamento della resilienza collettiva degli Stati membri, garantendo un'infrastruttura digitale sicura e con elevati standard di privacy, in cui i servizi pubblici e i servizi sanitari e assistenziali siano accessibile online per tutti.
Basandosi sulla bussola per il digitale 2030, la Commissione ha delineato il citato meccanismo di cooperazione annuale con gli Stati membri attraverso i seguenti strumenti:

- un sistema di monitoraggio strutturato, trasparente e condiviso, basato sull'indice di digitalizzazione dell'economia e della società (DESI) per misurare i progressi compiuti verso ciascuno degli obiettivi per il 2030;
- una relazione annuale sullo "stato del decennio digitale", in cui la Commissione valuterà i progressi compiuti e raccomanderà eventuali azioni;

- delle tabelle di marcia strategiche pluriennali per il decennio digitale per ciascuno Stato membro, in cui gli Stati membri delineeranno le politiche e le misure adottate o previste a sostegno degli obiettivi per il 2030;
- un quadro strutturato annuale per discutere e affrontare l'aspetto dei settori in cui i progressi sono insufficienti, con raccomandazioni e impegni congiunti tra la Commissione e gli Stati membri;
- un meccanismo per sostenere l'attuazione dei progetti multinazionali.

Proposta di decisione che istituisce un percorso per il decennio digitale

5. Risoluzione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale

L'uso sempre più frequente dell'Intelligenza Artificiale (IA) nel diritto penale si basa, in particolare, sulla promessa che ridurrà determinati tipi di reati (tra cui vengono menzionati nella Risoluzione del Parlamento reati finanziari, riciclaggio di denaro, finanziamento del terrorismo, abusi sessuali e sfruttamento sessuale nei confronti di minori online nonché alcuni tipi di reati informatici) e favorirà l'adozione di decisioni più obiettive.
Anche se il Parlamento europeo riconosce il contributo positivo di determinati tipi di applicazioni di IA al lavoro delle autorità di contrasto e giudiziarie in tutta l'Unione, esso prende atto con tale risoluzione del potenziale di rischio di tali strumenti per la protezione dei diritti fondamentali, elaborando una serie di raccomandazioni. Tra queste, si evidenzia come i sistemi di IA, per garantirne la sicurezza e la legittimità, debbano essere programmati, prodotti ed utilizzati secondo i principi di trasparenza, spiegabilità, non discriminazione, contestabilità e tracciabilità dei processi e dei risultati raggiunti. Principi che si accompagnano alla concezione di un'IA *human-centric*, secondo cui i sistemi di IA dovrebbero essere progettati in modo che possano essere sempre disattivati da un operatore umano.
Il Parlamento evidenzia come l'impiego delle applicazioni di IA da parte delle autorità di polizia e contrasto debba essere classificato come ad alto rischio. Inoltre, il suo sviluppo, la sua diffusione e il suo utilizzo dovrebbero essere soggetti a una continua valutazione dei rischi e a una rigorosa verifica della necessità e della proporzionalità. Si raccomanda invece l'esplicito divieto di determinati utilizzi di sistemi di IA, come quelli che potrebbero risultare in sorveglianza di massa, nuocere all'integrità fisica degli esseri umani, attribuire diritti o imporre obblighi giuridici agli individui, così come l'uso dell'IA e delle relative tecnologie per l'emanazione di decisioni giudiziarie. Il Parlamento chiede infine un divieto di utilizzo di database privati di riconoscimento facciale per le attività di contrasto.
Si invita ad applicare con coerenza il principio di precauzione per tutte le applicazioni di IA nel contesto delle attività di contrasto, sottolineando che la responsabilità giuridica e l'imputabilità devono sempre ricadere su una persona fisica o giuridica, identificata per le decisioni assunte con il sostegno dell'IA.
Con riguardo ad alcune specifiche applicazioni, il Parlamento evidenzia che l'utilizzo di tecniche di c.d. polizia predittiva, se da un lato permette di analizzare gli insiemi di dati forniti per l'identificazione di modelli e correlazioni, dall'altro non può dare una risposta alla questione della causalità, non può fare previsioni affidabili sui comportamenti degli individui e pertanto non può costituire l'unica base per un intervento.

Risoluzione del Parlamento europeo del 6 ottobre 2021 (2020/2016(INI))

6. Risoluzione del Parlamento europeo sullo stato della capacità di ciberdifesa dell'Unione Europea

Con la sottoindicata Risoluzione il Parlamento Europeo formula inviti e osservazioni per il miglioramento della capacità della ciberdifesa dell'Unione, evidenziando come la natura senza frontiere del ciberspazio, nonché l'elevato numero e la crescente complessità degli attacchi informatici richiedano una risposta coordinata a livello dell'Unione, che comprenda capacità comuni di sostegno degli Stati membri ed una cooperazione intensificata con la NATO, per affrontare insieme le sfide delle tecnologie emergenti e le minacce agli interessi della sicurezza euro-atlantica.
Viene sottolineato come sia essenziale superare l'attuale frammentazione dell'architettura informatica globale all'interno dell'UE, sviluppando una visione comune riguardo a come conseguire la sicurezza e la stabilità nel

ciberspazio incentrata sulla cultura della condivisione delle informazioni e dello scambio delle migliori pratiche.
A tal fine si raccomanda l'istituzione di un'unità congiunta così da garantire una rete d'informazione sicura e rapida che sappia sfruttare la cifratura dei dati. Dato il frequente carattere "a duplice uso" delle cibertecnologie, si invitano, inoltre, la Commissione e gli Stati membri ad adottare sistemi di certificazione per i prodotti, i servizi e i processi TIC al fine di innalzare il livello complessivo della cibersicurezza all'interno del mercato unico digitale e migliorare la cooperazione con il settore privato ed in particolare con le entità coinvolte nella gestione di infrastrutture critiche.
Il Parlamento, riconoscendo che la ciberdifesa è più efficace se contempla anche una serie di misure restrittive mirate a scoraggiare e contrastare gli attacchi informatici, ne chiede l'ulteriore sviluppo a partire dalla decisione del Consiglio del 14 maggio 2019 e nel rispetto al contempo della visione europea di Internet quale rete neutrale e libera.
Incoraggia, inoltre, le Nazioni Unite a favorire il dialogo tra Stati, ricercatori, accademici, organizzazioni della società civile, attori umanitari e settore privato onde garantire processi inclusivi di definizione di nuove disposizioni internazionali nel ciberspazio. In proposito, ribadendo la sua posizione sul divieto di sviluppare, produrre e utilizzare armi completamente autonome, che consentano di sferrare attacchi senza un significativo intervento umano, chiede l'avvio di negoziati internazionali su uno strumento giuridicamente vincolante che vieti questo tipo di armi.

In generale il Parlamento chieda che l'UE assuma un ruolo guida nella promozione di un quadro normativo globale in materia di IA che sia ispirato ai valori democratici e conforme al diritto internazionale umanitario.

Risoluzione del Parlamento europeo del 7 ottobre 2021 (2020/2256(INI))

7. Conclusioni del Consiglio Europeo su un'unità congiunta per il ciberspazio a integrazione della risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala

In data 19 ottobre 2021 il Consiglio ha adottato conclusioni con le quali invita l'UE e gli Stati membri a sviluppare ulteriormente il quadro dell'UE per la gestione delle crisi di cibersicurezza, esplorando il potenziale di un'unità congiunta per il ciberspazio proposta dalla Commissione il 23 giugno 2021.
Ribadendo la competenza esclusiva in materia di sicurezza nazionale degli Stati membri, compreso il settore della cibersicurezza, sottolinea la necessità di evitare inutili duplicazioni, garantendo, da un lato, il coordinamento con i meccanismi, le iniziative, le reti, i processi e le procedure esistenti a livello nazionale ed europeo, rafforzando, dall'altro, la cooperazione e la condivisione delle informazioni tra le varie cibercomunità all'interno dell'UE e dei suoi Stati membri a tutti i livelli.
In particolare, l'istituzione di un'unità congiunta per il ciberspazio dovrebbe fungere da strumento integrativo, secondo un processo graduale e trasparente, rispettoso dei ruoli e delle competenze degli Stati membri, degli organi e delle agenzie dell'UE, nonché dei principi di proporzionalità, sussidiarietà, inclusività, complementarità, non duplicazione e riservatezza delle informazioni.
A tal fine per il Consiglio l'unità dovrebbe essere costituita partendo da una mappatura approfondita delle possibili lacune ed esigenze, compresa una valutazione dei compiti e dei ruoli assegnati all'ENISA, per poi concordare possibili priorità e tempistiche entro cui raggiungerle.

Esplorare il potenziale dell'iniziativa concernente un'unità congiunta per il ciberspazio

8. Report FAFT-GAFI sui benefici della tecnologia nella prevenzione del riciclaggio e del finanziamento del terrorismo

In data 27 ottobre 2021 è stato presentato il report che riassume i risultati chiave del progetto congiunto condotto dal FAFT-GAFI e dal Gruppo Egmont, quale organismo globale delle Financial Intelligence Unit (FIU), sulle tipologie di strumenti digitali da impiegare nell'analisi dei flussi finanziari per ottimizzare la prevenzione del riciclaggio e del finanziamento del terrorismo (AML/CFT).

È messo in particolare in evidenza come sistemi di machine learning e d'Intelligenza Artificiale consentano di trattare immensi volumi di dati, raggiungendo una parziale automatizzazione del processo di analisi con identificazione più rapida dei rischi emergenti. Con riferimento allo scambio d'informazioni relative alle segnalazioni di operazioni sospette tra le varie Financial Intelligence Unit nazionali, nonché con i soggetti segnalanti e le autorità nazionali ed internazionali competenti, è stato evidenziato, invece, come l'impiego di strumenti digitali garantisca una trasmissione più sicura, a tutela della privacy.

Digital Transformation of AML/CFT for Operational Agencies

9. Aggiornamento FAFT-GAFI sui Virtual Assets (VA) and Virtual Assets Service Providers (VASP)

In data 28 ottobre 2021 è stato pubblicato l'aggiornamento della Guida relativa all'analisi dei rischi di riciclaggio e finanziamento del terrorismo (AML/CFT) relativa ai Virtual Assets e ai Virtual Assets Service Providers.
In particolare viene esaminato come intendere e applicare le raccomandazioni FAFT-GAFI ai relativi soggetti e attività, definendo anche l'approccio che dovrebbe essere adottato dai paesi e dalle autorità competenti mediante esempi di soluzioni regolamentari, nonché indicazioni per la cooperazione internazionale.
Nell'allegato A viene riportato il testo aggiornato della Raccomandazione 15 e la sua nota interpretativa, nella quale sono sintetizzate i risultati della verifica, mettendo in rilievo in particolare la necessità che sia prevista per i VASP una licenza o registrazione nel paese di origine o in quello di attività e che siano previste misure ad hoc che impediscano ai criminali di averne il controllo o detenerne anche solo una partecipazione. Si suggerisce anche la previsione di sanzioni, siano esse penali, civili o amministrative, sia per i VASP che operino senza le licenze-autorizzazioni del caso, sia per quelli che non rispettino i requisiti e gli obblighi della disciplina di prevenzione del riciclaggio e del finanziamento del terrorismo. In proposito si consiglia anche la creazione di appositi sistemi di monitoraggio e supervisione, con designazione di un'autorità competente munita di poteri, come quello ispettivo, di richiesta di informazioni e sanzionatorio, compresa la possibilità di revocare, limitare o sospendere la licenza o la registrazione.
A questa autorità dovrebbe essere anche consentito d'interfacciarsi e scambiare informazioni con le controparti estere, a prescindere dalla loro natura e dalle differenze regolamentari relative alla disciplina applicabile ai VASP, al fine di consentire una più efficace azione di contrasto del riciclaggio e del finanziamento del terrorismo, nonché dei reati presupposti.
In proposito è ribadito come la strumentalizzazione illecita della natura transfrontaliera dei Virtual Assets, impiegati come riscatti in attacchi ransomware, per truffe e traffici di stupefacenti o armi, in tratte di essere umani, richieda l'introduzione di una disciplina globale di prevenzione del riciclaggio e del finanziamento del terrorismo, che dovrebbe essere affiancata ad altri interventi regolamentari a tutela di consumatori ed investitori.

Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers

10. Proposta della Commissione per aumentare la cibersicurezza dei dispositivi senza fili

In data 29 ottobre 2021 la Commissione Europea ha presentato una proposta di atto delegato relativo alla direttiva sulle apparecchiature radio 2014/53/EU per aumentare la cibersicurezza dei dispositivi senza fili disponibili sul mercato europeo. Le misure proposte riguardano, in particolare, telefoni cellulari, tablet, fotocamere e altri prodotti in grado di comunicare via Internet, giocattoli e apparecchiature per l'infanzia, rispetto alle quali risulta centrale la tutela dei diritti dei minori, nonché una serie di apparecchiature indossabili, come gli smartwatch o i fitness tracker.
Si tratta di prescrizioni relative alla progettazione e alla produzione dei prodotti interessati al fine di: 1. evitare che questi dispositivi danneggino le reti di comunicazione o alterino la funzionalità di siti web o di altri servizi; 2. garantire la privacy impedendo l'accesso o la trasmissione non autorizzati di dati personali; 3. ridurre il rischio di frode nei pagamenti elettronici mediante un migliore controllo dell'autenticazione dell'utente.

Se il Parlamento europeo e il Consiglio non solleveranno entro due mesi obiezioni, l'atto delegato sarà pubblicato nella Gazzetta Ufficiale dell'Unione come regolamento e inizierà a decorrere un periodo transitorio di 30 mesi per l'adeguamento dei settori interessanti.

DELEGATED REGULATION (EU) of 29.10.2021 supplementing Directive 2014/53/EU

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Abusivismo finanziario: più di 500 Siti web oscurati da CONSOB

In poco più di due anni, da luglio 2019, quando è divenuto operativo il potere interdittivo conferito all'Autorità italiana per la vigilanza dei mercati finanziari con la legge n. 58 del 28 giugno 2019, articolo 36, Consob ha emesso oltre 500 provvedimenti con cui ha richiesto ai fornitori di servizi di connettività Internet d'inibire l'accesso dall'Italia ai siti web che offrono servizi finanziari senza la dovuta autorizzazione. Nel diffondere la notizia l'Autorità ha richiamato i risparmiatori sulla necessità che essi adottino alcune imprescindibili pratiche per assicurarsi investimenti in sicurezza, quali la verifica preventiva, per i siti che offrono servizi finanziari, che l'operatore tramite cui si investe sia autorizzato e, per le offerte di prodotti finanziari, che sia stato pubblicato il prospetto informativo.

Comunicato stampa Consob del 17 settembre 2021

2. La nuova disciplina per l'acquisizione dei tabulati telefonici

Nella Gazzetta Ufficiale del 30 settembre 2021, n. 234 è stato pubblicato il decreto-legge n. 132/2021, recante «*Misure urgenti in materia di giustizia e difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP*». L'art. 1 di tale norma ha modificato in modo significativo la disciplina dell'art. 132 del d.lgs. 196/2003 c.d. 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. In particolare, la possibilità di acquisizione dei tabulati telefonici e informatici è stata limitata 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, e ai reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo siano gravi. Inoltre, è stato previsto che tali dati siano acquisiti con decreto motivato del giudice su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private. Solo nei casi di urgenza è possibile per il pubblico ministero acquisire direttamente tali dati, ma in questo caso è necessaria la successiva convalida del giudice.

Decreto-Legge 30 settembre 2021, n. 132 - Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP

Sulle novità in tema di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale è stata pubblicata la Relazione n. 55/2021 dell'Ufficio del Massimario presso la Corte di cassazione.

Per approfondire: MALACARNE A., *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, in *Sist. Pen*., 8 ottobre 202; 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 CADOPPI A., CANESTRARI S., MANNA A. e PAPA A. (a cura di), *Cybercrime*, 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; ID., *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; ID., *Le recenti sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională *sul* data retention, in VIOLANTE L., GALIANI T., MERLI A. (a cura di), *Oggetto e limiti del potere coercitivo dello Stato nelle democrazie costituzionali. Annali della facoltà giuridica*, Camerino, 2013, p. 308 ss.

3. Segnalazioni al Garante per la protezione dei dati personali di casi di pornografia non consensuale

Con l'articolo 9 comma 1 lett. e) del decreto legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali, si inserisce il nuovo articolo 144-bis nel codice della privacy (d.lgs. 30 giugno 2003, n. 196). Tale nuova disposizione prevede che chiunque, compresi i minori ultraquattordicenni, abbia fondato motivo di ritenere che immagini o video a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione senza il suo consenso in violazione dell'art. 612-ter del codice penale, può rivolgersi, mediante segnalazione o reclamo, al Garante, il quale, entro quarantotto ore dal ricevimento della richiesta, dovrà avviare le indagini secondo quanto previsto dall'articolo 58 del GDPR e dagli articoli 143 e 144 del codice privacy.
Quando le immagini o i video riguardano minori, la richiesta al Garante può essere effettuata anche dai genitori o dagli esercenti la responsabilità genitoriale o la tutela. A chiusura della norma si dispone che l'invio, a tal fine, al Garante di immagini o video a contenuto sessualmente esplicito riguardanti soggetti terzi, effettuato dall'interessato, non integra il reato di cui all'articolo 612-ter del codice penale.

Decreto legge 8 ottobre 2021, n. 139

4. Parere Commissione Giustizia sullo schema del decreto legislativo di attuazione della direttiva sulla lotta al riciclaggio mediante il diritto penale

La Commissione parlamentare Giustizia, nel rilasciare, in data 20 ottobre 2021, parere favorevole sullo schema del decreto legislativo di recepimento della direttiva UE/2018/1673 sulla lotta al riciclaggio mediante il diritto penale (per la cui analisi si rinvia alla newsletter di agosto/settembre), ha espressamente richiesto di valutare la previsione, anche con riferimento ai reati di riciclaggio, di disposizioni ad hoc relative alle cripto-valute, quali beni che "*possono costituire condotte di riciclaggio*".

Parere Commissione Giustizia 20 ottobre 2021

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Adescamento di minori e detenzione di materiale pedopornografico

Nella sottoindicata pronuncia la Corte di Cassazione ribadisce che il reato di detenzione di materiale pedopornografico di cui all'art. 600-quater c.p. ha natura permanente, la cui consumazione inizia nel momento in cui il reo si procura il materiale e cessa nel momento in cui quest'ultimo ne perde la disponibilità. Mentre non fa cessare la detenzione la cancellazione di *files* pedopornografici, scaricati da Internet, mediante

l'allocazione nel "cestino" del sistema operativo del computer, in quanto gli stessi restano comunque disponibili mediante la semplice riattivazione dell'accesso al file. Solo per i files definitivamente cancellati può dirsi cessata la disponibilità e, quindi, la detenzione.
Per quanto riguarda invece il diverso reato di adescamento di minori previsto dall'art. 609-undecies c.p., seppur l'imputato avesse richiesto al minore la produzione di foto che non potevano essere ritenute di natura pedopornografica, la direzione finalistica di tale condotta alla produzione di materiale pedopornografico è stata ricavata dalla Corte da numerosi elementi che dimostravano come l'imputato, facendo leva sui sogni del giovanissimo calciatore e spacciandosi falsamente per procuratore calcistico, avesse nei suoi confronti tenuto una condotta di artifici e lusinghe volti a carpirne la fiducia, con proposta di incontrarlo per un colloquio e di ospitarlo per la notte a casa propria. Il dolo specifico richiesto dalla norma non deve infatti necessariamente risultare manifesto da quanto esplicitato con la condotta direttamente posta in essere nei confronti del minore, ben potendo la relativa prova essere ricavata anche *aliunde*. Ed invero se l'imputato avesse richiesto al minore fotografie riproducenti i propri organi sessuali, avrebbe commesso il più grave reato di tentata produzione di materiale pedopornografico, circostanza che, per la clausola di riserva che apre l'art. 609-undecies c.p., ne avrebbe impedito l'applicazione.

Conformi: Corte di Cassazione, sez. III penale, 15 aprile 2016 (ud. 23 febbraio 2016) n. 15719/2016, Pres. Fiale – Rel. Andreazza; Corte di Cassazione, sez. III penale, 8 marzo 2017 (ud. 7 aprile 2016) n. 11044/2017, Pres. Rosi – Rel. Gentili.

Per approfondire: PICOTTI L., *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in M. BERTOLINO e G. FORTI (a cura di), *Scritti per Federico Stella*, Napoli, 2007, vol. II, p. 1267 ss.; I. SALVADORI, *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata*, Napoli, 2016; ID., *L'adescamento di minori: Il contrasto al child-grooming tra incriminazione di atti preparatori ed esigenze di garanzia*, Torino, 2018.

Corte di Cassazione, sez. III penale, 2 settembre 2021 (ud. 20 aprile 2021), n. 32639/2021, Pres. Aceto – Rel. Reynaud

2. Sul dolo specifico del reato di adescamento di minori

Il dolo specifico del reato di adescamento di minori, consistente nell'intenzione di commettere i reati di cui agli artt. 600, 600-bis, 600-ter e 600-quater c.p., non deve necessariamente risultare manifesto da quanto esplicitato nella condotta direttamente posta in essere nei confronti del minore, ben potendo la relativa prova essere ricavata anche aliunde e ricorrendo il diverso reato di tentata prostituzione minorile ove il soggetto agente prospetti con chiarezza al minore il proposito di compiere con lo stesso atti sessuali con promessa di un compenso od un'utilità.
Essendo poi il reato di adescamento di pericolo indiretto, a tutela anticipata della integrità sessuale dei minori, sussiste prima ancora che gli atti possano considerarsi idonei e diretti in modo non equivoco a commettere il reato scopo, come in presenza di una sola richiesta d'invio via chat di foto del minore nudo, e si configura anche nei confronti di minore eventualmente già con esperienze sessuali.

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; BOGGIANI M., *L'adescamento di minorenni*, in CADOPPI A., CANESTRARI S., MANNA A. e PAPA A. (a cura di), *Cybercrime*, Torino, 2019, p. 599 ss.; PICOTTI L., *La pedopornografia nel Cyberspace: un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale riflessi nell'evoluzione normativa*, in *Diritto di Internet*, 2019, n. 1, p. 177 ss.; SALVADORI I., *I minori da vittime ad autori di reati di pedopornografia? Sui controversi profili penali del sexting*, in *Ind. pen.*, 2017, n. 3, 789 ss.; SALVADORI I., *L'adescamento di minori. Il contrasto al child-grooming tra incriminazione di atti preparatori ed esigenze di garanzia*, Torino, 2018; PICOTTI L., *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in BERTOLINO M. e FORTI G. (a cura di), *Scritti per Federico Stella*, Napoli 2007, vol. II, p. 1267 ss.

In generale, sulla differente struttura dei reati a dolo speciifco rispetto alla struttura deel tentativo, cfr. PICOTTI L., *Il dolo specifico. Un'indagine sugli elementi finalistici delle fattispecie penali,* Giuffrè, 1993, in specie pagg. 511-520.

Cass. pen, sez. III, 28 settembre 2021 (ud. 6 luglio 2021) n. 35625/2021, Pres. Di Nicola- Rel. Socci

3. *Sexting* e reato di detenzione di materiale pedopornografico

La Corte di Cassazione non ritiene riconducibile il caso esaminato al controverso concetto di c.d. pedopornografia "domestica", ossia alle ipotesi di materiale pedopornografico "auto-prodotto" (*sexting*), sulla cui rilevanza penale si è creato un ricco dibattito giurisprudenziale, culminato in una recente ordinanza di remissione della questione alle Sezioni Unite (cfr. Newsletter OC luglio-agosto 2021), dal momento che le fotografie venivano effettuate dall'imputato condizionando quello che poteva apparire un consenso del minore, il quale veniva pagato dall'imputato per avere rapporti sessuali. La Corte ha quindi ritenuto sussistente il reato di detenzione di materiale pedopornografico ex art. 600-quater c.p.. Nella pronuncia, peraltro, si evidenzia quale preferibile quell'orientamento giurisprudenziale secondo cui le condotte illecite previste dal codice penale aventi ad oggetto materiale pedopornografico, diverse da quella di produzione dello stesso punita dall'art. 600-ter, comma 1, n. 1, seconda parte, c.p., non presuppongono necessariamente la commissione di tale reato, potendo essere configurabili anche nel caso in cui detto materiale sia stato realizzato dallo stesso minore. Il richiamo al "materiale pornografico realizzato utilizzando minori degli anni diciotto", contenuto nell'art. 600-quater, comma 1, c.p., deve quindi essere inteso con esclusivo riguardo alla oggettiva natura pedopornografica della rappresentazione, nel senso oggi codificato nell'art. 600-ter u.c., c.p., sicché i reati sussistono anche nel caso in cui si tratti di materiale autoprodotto dallo stesso minore.

Conformi: Corte di Cassazione, sez. III penale, ordinanza 1° luglio 2021 (ud. 22 aprile 2021), n. 25334 - Pres. Marini, Rel. Rosi; Corte di Cassazione, sez. III penale, 12 febbraio 2020 (ud. 21 novembre 2019) n. 5522/2020, Pres. Izzo - Rel. Macrì; 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*, in *Dir. di Internet*, 2019, n. 1, p. 177 ss.; Corte di Cassazione, sez. V penale, sentenza 19 luglio 2018 (ud. 8 giugno 2018), n. 33862/2018, Pres. Sabeone – Rel. Tudino.

Per approfondire: ROSANI D., *Cessione di immagini pedopornografiche autoprodotte ('selfie'): la Cassazione rivede la propria lettura dell'art. 600-ter c.p.*, in *Sistema penale*, 4 dicembre 2020; ID., «Send nudes». *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, 6 ottobre 2021 (ud. 11 giugno 2021), n. 36198/2021, Pres. Rosi - Rel. Reynaud.

4. Sostituzione di persona e *social network*

L'imputato, effettuando l'accesso a un profilo Facebook originariamente aperto della persona offesa e modificando la password per impedirne l'accesso a terzi, pubblicava link pornografici, che, ai frequentatori della rete, apparivano riconducibili al profilo Facebook che lo stesso imputato aveva provveduto a rinominare in modo da associare le immagini pornografiche da lui immesse sul profilo alla vittima. L'affermazione di responsabilità dell'imputato per il reato di cui all'art. 494 c.p. si inserisce dunque all'interno di un consolidato orientamento della giurisprudenza di legittimità, secondo cui integra il reato di sostituzione di persona la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete internet e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, includendolo subdolamente in una corrispondenza idonea a lederne l'immagine e la dignità.

Conformi: *ex multis*, Corte di Cassazione, sez. V penale, 23 luglio 2020 (ud. 6 luglio 2020), n. 22049/2020, Pres. Palla – Rel. Riccardi.

Per approfondire: CRESCIOLI C., *Profili penali dellae della persona*, in *Dir. inf.*, 2008, p. 526 ss.; PICOTTI L., *Profili penali delle comunicazioni illecite via Internet*, in *Dir. inf.*, 1999, p. 283 ss.

Corte di Cassazione, sez. V penale, 20 settembre 2021 (ud. 15 giugno 2021), n. 34813/2021, Pres. Miccoli - Rel. Guardiano

5. Sostituzione di persona via mail

Sussiste il reato di sostituzione di persone nell'invio ad un avvocato difensore di terzi di messaggi di posta elettronica da indirizzo mail, appositamente creato, riportante i dati del cliente e recante la sua apparente firma.

Per la Corte si tratta di modalità idonea ad ingannare, che ha, infatti, in concreto tratto in errore l'avvocato in questione, indipendentemente e a prescindere dalla circostanza che il destinatario per la sua qualità professionale avesse avuto gli strumenti per accorgersi dell'inganno o che avesse il dovere di prestare più attenzione in ordine alla provenienza del messaggio, prima di rispondere sullo stato dei procedimenti processuali.

Per approfondire: CORBETTA S., *Falsa creazione di un profilo facebook: è sostituzione di persona*, nota a Cass. pen., sez. V, sentenza 23/07/2020, n. 2204, in *Diritto penale e processo*, 2020, n. 9, p. 1182 ss., ID., *Falsa creazione di un profilo su un social network: è sostituzione di persona*, nota a Cassazione penale, sez. V, sentenza 16/06/2014, n. 25774, in *Diritto penale e processo*, 2014, n. 7, p. 810 ss.; CRESCIOLI C., *Una sentenza della Cassazione sulla sostituzione di persona* online, in *Dir. pen. cont.*, 21 giugno 2019; MALAGNINO F., *Sostituzione di persona e web: le false recensioni online*, in *Giurisprudenza penale*, 2019, n. 4, p. 1 ss.; STAMPANONI BASSI G., *In tema di sostituzione di persona commessa nella rete*, nota a Cass. pen., sez. V, sentenza 29/04/2013, n. 18826, in *Cassazione penale*, 2014, n. 1, p. 146 ss..

Cass. Pen., sez. V, 16 settembre 2021 (ud. 28 maggio 2021), n. 34468/2021, Pres. Rossella- Rel. Mauro.

6. Accesso abusivo e recidiva

Con riguardo al reato di accesso abusivo al sistema informatico del Comune di Firenze, realizzato mediante impiego delle password di colleghe di lavoro assenti dall'ufficio da soggetto indagato per diverse casi di truffa aggravata ai danni dello Stato, l'attualità del rischio di reiterazione di reati analoghi- ai fini dell'applicazione della recidiva in sede cautelare-può essere tratta dalla connotazione complessiva della condotta, ancorché arrestatasi due anni or sono a seguito della perquisizione e del sequestro del materiale informatico nella sua disponibilità, in quanto costituita da diversi episodi ripetuti più volte nel corso del tempo ed accomunati dalla strumentalizzazione della funzione a fini personali, segno di un impulso delinquenziale non episodico.

Per approfondire: PENCO E., *Offensività e colpevolezza nel controllo di costituzionalità in materia di recidiva e giudizio di bilanciamento*, in *Diritto penale e processo*, 2021, n. 2, p. 260 ss.; SALVADORI I., *I reati contro la riservatezza informatica*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Torino, 2019, p. 656 ss.; FLOR R., *La condotta del pubblico ufficiale fra violazione della* voluntas domini*, "abuso" dei profili autorizzativi e "sviamento di poteri"*, in *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.; ZAMPERINI V., *Impugnabilità del sequestro probatorio di dati informatici*, in *Diritto penale e processo*, 2016, *n.* 4, *p.* 509 ss..

Corte di Cassazione, sez. V penale, 13 settembre 2021 (ud. 9 luglio 2021), n. 33878, Pres. Pezzullo- Rel. Borrelli

7. Limiti nell'accertamento probatorio di responsabilità penali per reati realizzati in rete

Con la sottoindicata pronuncia la Corte di Cassazione dispone l'annullamento con rinvio della sentenza impugnata che aveva assolto l'imputato per non aver commesso i reati di cui agli artt. 81, 609-quater, 609-bis e 609-ter, 610, 615-ter, 494 e 612-bis c.p. in virtù dell'insufficiente forza probatoria di taluni elementi indiziari. Tali reati, in ipotesi d'accusa, sarebbero stati commessi in esecuzione del medesimo disegno criminoso, ed erano stati ascritti per aver l'imputato contattato, per mezzo di falsi profili Facebook, una minore di anni quattordici, dapprima inducendola a mostrarsi nuda e a compiere atti di autoerotismo, costringendola poi a proseguire in tali condotte, con la minaccia di divulgare i video, e a fornirgli le password dei suoi profili *social*, così introducendovisi e sostituendosi alla minore, in questo modo diffondendo ai di lei parenti e conoscenti i video pornografici che la ritraevano. La Corte di legittimità evidenzia come siano stati svalutati, tra i vari elementi riportati, il fatto che una delle linee telefoniche utilizzate dall'autore del reato fosse intestata all'imputato, così come l'utilizzo da parte dell'imputato di un dato programma informatico, osservando come lo stesso avesse anche altre utilità, oltre ad impedire *ex post* l'accertamento dell'uso che del computer viene fatto, senza in alcun modo confrontarsi con gli assunti della sentenza di primo grado circa il suo normale impiego, soprattutto in strutture professionali, e circa la sua immediata (e, quanto ai tempi, sospetta) installazione nel nuovo *hard disk* che l'imputato si procurò successivamente al sequestro del primo computer. Infine la Corte territoriale non ha in alcun modo preso in considerazione l'abilità e l'interesse dell'imputato per gli apparecchi informatici e la frequenza di utilizzo degli stessi da parte sua.

Corte di Cassazione, sez. III penale, 14 ottobre 2021 (ud. 15 giugno 2021), n. 37384/2021, Pres. Di Nicola - Rel. Reynaud.

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

Rosani D., *Sexting minorile: le Sezioni unite chiamate ad esprimersi sul materiale pedopornografico prodotto col consenso del minore (600-ter c.p.)*, 29 settembre 2021

Malacarne A., *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, 8 ottobre 2021

Diritto di Internet n. 4/2021

Pizzetti F., L*a proposta di regolamento sull'IA della commissione europea presentato il 21.4.2021 (COM (2021) 206 final) tra mercato unico e competizione digitale globale*, p. 591 ss.

Malacarne A., *Il ricorso a strumenti investigativi a cd. contenuto tecnologico. la data retention nel procedimento penale alla luce della giurisprudenza europea e della (ondivaga) giurisprudenza di merito italiana*, p. 609 ss.

La Rosa A., *La responsabilità del gestore di una piattaforma di condivisione di video o di una piattaforma di hosting e di condivisione di file ai sensi della direttiva 2000/31/CE. Rilevanza dell'inerzia "informata"*, Nota a *Corte di giustizia UE, Grande sezione, sentenza 22 giugno 2021, cause riunite C-682/18 e C-683/18*, p. 622 ss.

Altre riviste e contributi

Vadalà R.M., *La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale*, nota a Cass. pen., Sez. II, 25 settembre 2020, n. 26807, in *Giurisprudenza Italiana*, 2021, n. 10, p. 2224 ss.

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.

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