News febbraio 2021

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

NOVITÀ SOVRANAZIONALI

1. Opinione n. 1/2021 del Garante europeo della protezione dei dati sulla proposta del *Digital Service Act*

Il garante europeo per la protezione dei dati personali (GEPD), richiamando anche sue precedenti osservazioni (Opinione n. 3/2018 sulla manipolazione online e i dati personali), ha identificato ed evidenziato la presenza di innumerevoli rischi per la protezione dei diritti fondamentali (ma anche della società nel suo complesso) collegati al contesto delle piattaforme online. In particolare, creando quella che è stata definita l'"economia dell'attenzione" (in cui i servizi sono disegnati per massimizzazione l'attenzione e la partecipazione dei consumatori), gli esistenti *advertising-driven business models* di molti servizi online hanno contribuito ad aumentare fenomeni di polarizzazione e manipolazione politica ed ideologica, la cui portata viene amplificata dall'utilizzo di sistemi algoritmici. A fronte di tale scenario, il GEPD accoglie favorevolmente la proposta della Commissione europea per un *Digital Service Act,* improntato alla promozione dei principi di trasparenza e responsabilizzazione delle piattaforme. Tuttavia, a parere del garante europeo, risultano necessarie alcune precisazioni o integrazioni in merito ad alcuni punti della proposta, che si coordino e tengano conto anche delle previsioni contenute nella proposta del *Digital Market Act.* Tra questi si segnala la necessità di: introdurre misure per garantire la complementarietà delle nuove previsioni con quelle già previste dal GDPR e dalla direttiva 2002/58/EC (direttiva relativa alla vita privata e alle comunicazioni elettroniche); fornire una definizione più specifica di legittimo trattamento di dati personali nell'ambito delle misure implementate dalle piattaforme per il contrasto ai contenuti illegali; intensificare la trasparenza nell'informativa che si dovrà fornire agli utenti in caso di utilizzo di strumenti automatici per le operazioni di moderazione dei contenuti; specificare (attraverso ad esempio la predisposizione di un allegato) quali siano i reati rilevanti per l'obbligo di notifica all'autorità previsto dall'art. 21 della proposta di regolamento.

Opinione n. 1/2021 del Garante europeo della protezione dei dati

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Newsletter del Garante per la protezione dei dati personali

Il Garante ha sottolineato il divieto di utilizzare le impronte digitali dei dipendenti per l'utilizzo di un sistema di rilevazione delle presenze in assenza di specifica previsione di legge. Infatti, a seguito del rafforzamento delle garanzie previste dal Regolamento GDPR e dal Codice privacy, per installare questo tipo di sistemi è necessaria una base normativa che sia proporzionata all'obiettivo perseguito e che fissi misure appropriate e specifiche per tutelare i diritti degli interessati. Pertanto, ha sanzionato per 30.000 euro l'Azienda sanitaria provinciale di Enna, che utilizzava tale sistema, sottolineando che la base normativa invocata era carente, non essendo stato adottato il regolamento attuativo della legge 56/2019 (poi abrogata) che doveva stabilire garanzie per circoscrivere gli ambiti di applicazione e regolare le principali modalità del trattamento.

Newsletter del Garante per la protezione dei dati personali n. 473 del 19 febbraio 2021

2. La sanzione dell'Autorità Garante della Concorrenza e del Mercato nei confronti di Facebook

Con provvedimento n. 27432 del 29 novembre 2018, l'Autorità Garante della Concorrenza e del Mercato (AGCM) aveva accertato che Facebook Inc. e Facebook Ireland Ltd. ponevano in essere una pratica commerciale scorretta, inducendo ingannevolmente gli utenti consumatori a registrarsi sulla piattaforma senza informarli adeguatamente, in fase di attivazione dell'*account*, dell'attività di raccolta, con intento commerciale, dei dati da loro forniti e, più in generale, delle finalità remunerative che sottendono la fornitura del servizio di social network, enfatizzandone la sola gratuità. Con tale provvedimento l'AGCM, oltre

sanzionare il social network per 7 milioni, aveva vietato l'ulteriore diffusione della pratica commerciale e disposto la pubblicazione da parte di Facebook di una dichiarazione di rettifica.
A fronte del mancato adempimento da parte di Facebook, che, pur avendo eliminato il *claim* di gratuità in sede di registrazione alla piattaforma, ancora non forniva un'immediata e chiara informazione sulla raccolta e sull'utilizzo a fini commerciali dei dati degli utenti, l'Autorità ha aperto a gennaio 2020 un nuovo procedimento, che si è concluso con il provvedimento qui riportato, con il quale è stata irrogata nei confronti del social network una ulteriore sanzione di 5 milioni di euro.

Provvedimento AGCM 17 febbraio 2021

3. Prevenzione di fenomeni di criminalità finanziaria connessi con l'emergenza da Covid-19

Con questa comunicazione, ad integrazione di quella del 16 aprile 2020, l'UIF (Unità di Informazione Finanziaria per l'Italia) fornisce ai soggetti obbligati all'applicazione delle misure antiriciclaggio nuovi elementi utili per favorire la segnalazione delle operazioni sospette nel contesto della crisi economica innescata dalla pandemia da COVID-19.
Con specifico riferimento alle transazioni digitali, rispetto alle quali viene ribadita l'esigenza di contrastare il rischio di reati informatici e di attività fraudolente, sono prescritte alcune indicazioni specifiche.
E', in particolare, sollecitata, relativamente all'operatività realizzata attraverso i cd. "ATM evoluti", quali strumenti di pagamento basati, ad es., su app mobile, la strutturazione di adeguati strumenti di monitoraggio e l'introduzione di idonei limiti quantitativi per mitigare il rischio di utilizzo distorto delle nuove tecniche per finalità illecite. Relativamente alle transazioni in valute virtuali dirette verso il dark web per l'acquisto, anche, di farmaci non sicuri, è sottolineata l'importanza del ricorso a tecniche di blockchain forensics per agevolare il riconoscimento di eventuali sospetti. Sempre con riferimento alle valute virtuali e non solo, a fronte dello sviluppo dall'inizio della pandemia di piattaforme on line per la realizzazione di obiettivi di investimento o app di brokeraggio, è richiesto che l'operatività rilevante e continuativa dei clienti che mostrano di interfacciarsi con queste piattaforme sia attentamente vagliata alla luce dei presidi antiriciclaggio, al fine di valutare l'esistenza di profili meritevoli di segnalazione.

Comunicazione dell'Unità di Informazione Finanziaria per l'Italia dell'11 febbraio 2021

4. Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo

Obiettivo del documento ministeriale è fornire i principi guida per la realizzazione da parte delle istituzioni scolastiche d'interventi efficaci per comprendere, ridurre e contrastare gli episodi di bullismo, nonché promuovere anche un uso positivo e consapevole delle tecnologie digitali da parte dei più giovani per prevenire e contrastare situazioni di rischio online. Tra le indicazioni date vi sono sia azioni di prevenzione, per promuovere e preservare lo stato di salute ed evitare l'insorgenza di patologie e disagi, sia di procedure operative da adottare nelle situazioni di contesto più a rischio. È, inoltre, prevista anche l'istituzione di un Team Antibullismo, costituito dal personale scolastico e dalle relative professionalità che vi operano, e di un Team per l'Emergenza per favorire il coinvolgimento anche delle forze dell'ordine e dei servizi sanitari. È espressamente consentito, poi, l'inserimento nel Regolamento di istituto di possibili provvedimenti disciplinari che devono essere proporzionati ai fatti di bullismo commessi ed ispirati alla riparazione del danno e all'acquisizione di consapevolezza sul significato della propria condotta
Alle Linee Operative sono allegati: a) il "Protocollo di intervento per un primo esame nei casi acuti e di emergenza"; b) le "Raccomandazioni e responsabilità degli organi e del personale della scuola", suddivise per tipologia di destinatario; c) un modulo fac-simile di segnalazione di comportamento a rischio a Forze di Polizia o Autorità Giudiziaria.

Ministero dell'Istruzione, documento n. 18 del 13.02.21 e nota n. 482 del 18.02.2021

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. La natura probatoria dei messaggi “whatsapp”

I messaggi “whatsapp” e gli sms conservati nella memoria di un telefono cellulare hanno natura di documenti ai sensi dell'art. 234 c.p.p., sicché, non trovando applicazione né la disciplina delle intercettazioni, né quella relativa all'acquisizione di corrispondenza di cui all'art. 254 c.p.p., è legittima la loro acquisizione mediante mera riproduzione fotografica dello schermo del telefono cellulare sul quale gli stessi sono leggibili (il cd. “screenshot”).

In senso conforme: Corte di Cassazione, Sez. VI penale, sentenza 17 gennaio 2020 (ud. 12 novembre 2019) n. 1822/2020, Pres. Petruzzellis - Rel. Bassi.

Per approfondire: TORRE M., *WhatsApp e l'acquisizione processuale della messaggistica istantanea*, in *Diritto penale e processo*, 2020, n. 9, p. 1279; FELICIONI P., L*'acquisizione di contenuti e-mail e delle chat whatsapp tra intercettazioni e sequestro*, in *Rivista della Guardia di finanza*, 2019, n. 6, p. 1555; DEL COCO R., *L'utilizzo probatorio dei dati whatsapp tra lacune normative e avanguardie giurisprudenziali*, in *Processo penale e giustizia*, 2018, n. 3, p. 532; più in generale sulla possibile rilevanza penale della messagistica WhatsApp, cfr. PICOTTI L., *La violenza sessuale via whatsapp*, in *Diritto di Internet*, 2020, n. 4, p. 689.

Corte di Cassazione, Sez. V penale, sentenza 24 febbraio 2021 (ud. 01 dicembre 2020), n. 7206/2021, Pres. De Marzo - Rel. Brancaccio

2. Il concorso del delitto di ricettazione e d’indebito utilizzo di carta di credito

Risponde dei reati di ricettazione e di indebito utilizzo di carte di credito di cui all'art. 493 ter, comma 1, prima parte, c.p., il soggetto che, non avendo concorso nella realizzazione della falsificazione, riceve da altri carte di credito o di pagamento contraffatte e faccia uso di tale mezzo di pagamento; mentre risponde delle due autonome ipotesi di reato previste dall'art. 493 ter, comma 1, c.p., in concorso, l'autore della contraffazione che proceda anche all'utilizzo indebito di questo mezzo di pagamento.

In senso conforme: Corte di Cassazione, Sez. II penale, sentenza del 18 novembre 2019 (udienza 18 settembre 2019) n. 46652/2019, Pres. Cammino - Rel. Pardo

Per approfondire: DE AMICIS G., *Contrasti giurisprudenziali in tema di "ricettazione" di carte di credito*, in *Cassazione penale*, 2000, n. 9, p. 241; AMATO G., *Solo nei casi di "provenienza delittuosa" l'acquisto di carte di credito è ricettazione - La punibilità dell'illecito utilizzo esclude il ricorso con il reato di truffa*, in *Guida al diritto*, 2001, n. 29, p. 58; GALANTE A., *La tutela penale delle carte di pagamento*, in Cadoppi A., Canestrari S., Manna A. e Papa A. (a cura di), *Cybercrime*, Torino, 2019, p. 285 ss.

Corte di Cassazione, Sez. II penale, sentenza 17 febbraio 2021, (ud. 15 gennaio 2021) n. 6195/2021, Pres. Diotallevi - Rel. De Santis

3. L’indebito utilizzo di carta carburante ai sensi dell’art. 493 ter

È condotta punibile a titolo d’indebito utilizzo ai sensi dell’art. 493 ter c.p. l’inserimento in uno sportello bancomat di una carta carburanti. Trattandosi di carta di credito o di pagamento, il suo indebito utilizzo non costituisce ipotesi di reato impossibile per inidoneità dell'azione in quanto l’art. 493 ter c.p. punisce la condotta a prescindere dal conseguimento del profitto che è oggetto di dolo specifico.

Per approfondire: PICOTTI L., *Il dolo specifico. Un'indagine sugli “elementi finalistici” delle fattispecie penali*, Milano, Giuffré, 1993; SICCARDI I., *Il fine di profitto nei delitti contro il patrimonio*, in *Diritto Penale e Processo*, 2016, n. 3, p. 357; ROSSI B., *Per l’integrazione del reato di cui all’ art. 493-ter c.p. non occorre il conseguimento di un profitto o il verificarsi di un danno*, in *Cassazione penale*, 2019, n. 10, p. 3653 ss.; PEDULLA’ C., *L’idoneità dell’azione costitutiva del reato impossibile,* in *Cassazione penale*, 2019, n. 11, p. 3990.

Corte di Cassazione, Sez. II penale, sentenza 17 febbraio 2021 (ud. 27 gennaio 2021), n.6184/2021, Pres. Diotallevi - Rel. Perotti

4. Il sequestro probatorio dello *smartphone*

Con questa pronuncia la Corte di Cassazione ha ribadito la legittimità del sequestro probatorio di un supporto informatico, nel caso di specie uno *smartphone*, disposto per svolgere accertamenti sui dati in esso contenuti, nonostante la L. 18 marzo 2008, n. 48, nel modificare le disposizioni del codice di procedura penale, abbia previsto all'art. 254-*bis* c.p.p. la possibilità di estrarre copia degli stessi- con modalità idonee a garantire la conformità dei dati acquisiti a quelli originali - in quanto questa disciplina non impedisce di imporre un vincolo su tali cose, ma si limita a consentire la presentazione di una successiva richiesta di restituzione a norma dell'art. 263 c.p.p.

In senso conforme: Corte di Cassazione, Sez. VI penale, sentenza 5 marzo 2014 (ud. 12 febbraio 2014), n. 10618/2014, Pres. Conti – Rel. Aprile

Corte di Cassazione, Sez. I penale, sentenza 15 febbraio 2021 (ud. 10 novembre 2020), n. 5846/2021, Pres. Iasillo – Rel. Siani

5. I presupposti minimi per l'accertamento della condotta di "partecipazione" ad associazioni con finalità di terrorismo

In merito al reato di partecipazione ad associazioni con finalità di terrorismo ex art. 270-*bis* c. 2 c.p., la Corte evidenzia come vi siano due diversi orientamenti in merito all'individuazione dei presupposti minimi per poter ritenere provato l'effettivo inserimento del singolo agente in tali organizzazioni criminali. Secondo un primo orientamento, sorto nell'affrontare il caso della c.d. *Jihad* elettronica (cioè l'impiego dei *social media* per la manifestazione di opinioni inneggianti alla guerra santa, al martirio, alla commissione di atti terroristici o al confezionamento di armamenti), è sufficiente che la condotta ideologica del soggetto si sostanzi in seri propositi criminali volti a realizzare una delle finalità associative, o sia strumentale al consolidamento ed al rafforzamento dell'organizzazione. Questa interpretazione attribuisce alle attività di propaganda, apologia e proselitismo la capacità di orientare il consenso nell'ampia sfera della comunicazione virtuale, dove la "smaterializzazione" (intesa quale *deficit* di ricaduta nel mondo fisico degli effetti della condotta) costituisce il portato di modalità di estrinsecazione dei fatti delittuosi che non postula necessariamente una fenomenologia che incide la realtà fisica, ma la veicolano attraverso pervasivi strumenti di manipolazione comunicativa.

Secondo un diverso orientamento, invece, al quale aderisce la Corte in tale pronuncia, l'accertamento della partecipazione del singolo ad una struttura organizzativa di natura terroristica, non può non implicare la verifica della "bilateralità" della relazione, cioè della volontà del soggetto di aderire e di dare il proprio concreto supporto alla realizzazione degli obbiettivi del sodalizio, da un lato, e della consapevolezza da parte del gruppo criminale (anche mediata, riflessa e indiretta) di tale adesione, dall'altro.

Anche se la partecipazione ad un'associazione terroristica di matrice islamico-fondamentalistica è connotata da un modello organizzativo "debole", atipico, "liquido", aperto alle adesioni spontanee dei singoli, non implicanti atti di affiliazione o riconoscimenti formali, ma che spesso di "materializzano" attraverso il web, intrinsecamente dematerializzato, è indispensabile che la condotta dell'agente possa qualificarsi quale dimostrativa della reale aggregazione del singolo ad un gruppo organico, attraverso la propria "messa a disposizione" - grazie all'esistenza di un contatto operativo - alla realizzazione degli obiettivi dello stesso. Si deve dunque evitare, secondo la Corte, che l'estrema pericolosità del fenomeno terroristico di matrice islamico-fondamentalistica conduca a interpretazioni che non tengano in dovuta considerazione i principi generali di materialità e di offensività della condotta, nonché le categorie generali in tema di reato associativo, là dove postulano la prova di un inserimento "effettivo" del singolo nell'organizzazione criminale.

In senso conforme: Corte di Cassazione, Sez. VI Penale, sentenza 11 settembre 2018 (ud. 23 febbraio 2018), n. 40348/2018, Pres. Fidelbo - Rel. Silvestri; Corte di Cassazione, Sez. VI Penale, sentenza 29 marzo 2018 (ud. 19 dicembre 2017), n. 14503/2018, Pres. Paoloni - Rel. Silvestri.

Per approfondire: PICOTTI L., *Terrorismo e sistema penale: realtà, prospettive, limiti, i*n D*ir. Pen. Cont. Riv. Trim., 2*017, n. 1, p. 249 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.

Corte di Cassazione, Sez. VI penale, sentenza 11 febbraio 2021 (ud. 17 novembre 2020), n. 5471/2021, Pres. Fidelbo - Rel. Bassi

6. Reato di adescamento di minorenni e principio di offensività

Chiedendo l'imputato con ricorso di sollevare questione di legittimità costituzionale del reato di adescamento di minori di cui all'art. 609 *undecies* c.p. per contrasto con il principio di offensività, data l'anticipazione della soglia di punibilità operata dalla fattispecie, la Corte conferma il suo precedente orientamento per cui ritiene la questione di legittimità costituzionale manifestamente infondata. Integrando un reato di pericolo concreto e dovendo accertare il dolo specifico attraverso parametri oggettivi dai quali si deduca il movente sessuale della condotta, la norma punisce comportamenti idonei a mettere in pericolo un bene giuridico primario con una cornice edittale equa e proporzionalmente inferiore a quella dei reati fine. Nel caso di specie la condotta di "lusinghe" finalizzate alla commissione di reati in materia sessuale e/o di pornografia è stata ritenuta integrata dall'invio di vari messaggi, tramite WhatsApp, contenenti apprezzamenti alla minore, nonché di immagini e fotografie sessualmente esplicite.

In senso conforme: Corte di Cassazione, sez. III penale, sentenza 13 luglio 2018 (ud. 15/03/2018), n. 32170/2018, Pres. Di Nicola - Rel. Andronio.

Per approfondire: BIANCHI M., *I confini della repressione penale della pornografia minorile: la tutela dell'immagine sessuale del minore fra esigenze di protezione e istanze di autonomia***,** Torino, 2019; SALVAODRI I., *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, sentenza 9 febbraio 2021 (ud. 28 ottobre 2020), n. 5039/2021, Pres. Lapalorcia – Rel. Gai

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

Birritteri E., *Controllo a distanza del lavoratore e rischio penale*

Canzio G.*, Intelligenza artificiale, algoritmi e giustizia penale*

Delaiti F.*, Cripto-valute e abusivismo finanziario: cripto-analogia o interpretazione estensiva?*

Diritto di Internet n. 1/2021

Contaldo A., *La tutela della privacy del domicilio informatico e il diritto d'autore: un difficile bilanciamento*

D'Agostino L., *Offerte di criptoattività e abusivismo finanziario. I margini di rilevanza penale dell'esercizio non autorizzato di servizi di investimento*

Giordano M.T.*, Offerte di criptoattività e abusivismo finanziario. I margini di rilevanza penale dell'esercizio non autorizzato di servizi di investimento*

Gualazzi A., *Immagini indebitamente carpite e diffusione sul web: sulla rilevanza scriminante della difesa da "pericolo informatico"*

Malacarne A., *Le registrazioni di colloqui ad opera di uno degli interlocutori tra contrasti interpretativi ed evoluzione tecnologica*

Monzillo B., *Quale regime per le comunicazioni tra persone all'estero intercettate dal captatore informatico?*

Altre riviste

Sicignano G.J., *Gli obblighi antiriciclaggio degli operatori in moneta virtuale: verso l'autocertificazione per gli utenti della blockchain?*, in *Riv. Trim. Dir. Pen. Cont.*, 2020, n. 4, p. 146 ss.

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