News agosto-settembre 2020

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

NOVITÀ SOVRANAZIONALI

1. L'avvio ufficiale della Procura europea

Il 28 settembre 2020 si è insediata ufficialmente la Procura europea, organismo indipendente dell'Unione europea con sede a Lussemburgo con compiti di indagine e di perseguimento di reati lesivi degli interessi finanziari europei e composto da ventidue componenti, uno per ogni Stato partecipante (Austria, Belgio, Bulgaria, Cipro, Croazia, Estonia, Finlandia, Francia, Germania, Grecia, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Portogallo, Repubblica ceca, Romania, Slovacchia, Slovenia e Spagna). La Procura europea svolgerà indagini, eserciterà l'azione penale ed esplicherà le funzioni di pubblico ministero dinanzi agli organi giurisdizionali competenti degli Stati membri, sarà operativa al termine del 2020 ed i suoi componenti avranno un mandato di sei anni non rinnovabile.

Si evidenzia che la Procura europea è competente ad indagare e perseguire i reati che ledono gli interessi finanziari dell'Unione europea, ovvero i reati indicati nella direttiva (UE) 2017/1371 sulla protezione degli interessi finanziari dell'Unione, c.d. direttiva PIF, appena recepita dal legislatore italiano col D.lgs. n. 75 del 14 luglio 2020 (v. Sezione novità legislative e normative nazionali)

Comunicato stampa n. 118 del 28 settembre 2020 che la Corte di Giustizia dell'Unione europea

2. La Corte di Giustizia UE e il principio di libertà di accesso ad *Internet*

Questa pronuncia trae origine da due controversie che vedevano opposti la Telenor Magyarország Zrt. e il Nemzeti Média- és Hírközlési Hatóság Elnöke, ovvero il Presidente dell'Ufficio nazionale ungherese dei media e delle comunicazioni, in merito a due decisioni con le quali quest'ultimo aveva ingiunto alla Telenor di porre fine ad alcuni dei suoi servizi di accesso a Internet. Tale organo aveva avviato due procedimenti sanzionatori contro tale società, che commercializzava due pacchetti denominati *MyChat* e *MyMusic*. In particolare, si trattava di pacchetti che consentivano ai clienti sottoscrittori rispettivamente di acquistare un volume di dati di un gigabit e di utilizzarlo senza restrizioni fino al suo esaurimento accedendo liberamente alle applicazioni e ai servizi disponibili e di ascoltare musica *online* utilizzando alcune applicazioni e servizi radiofonici. Una volta esaurito il suddetto volume di dati, i clienti sottoscrittori potevano continuare ad utilizzare senza restrizioni alcune applicazioni specifiche, mentre alle altre e ai relativi servizi disponibili erano applicate misure di rallentamento del traffico. La Corte ungherese aveva così sottoposto tramite rinvio pregiudiziale la questione relativa alla compatibilità di tali pacchetti col disposto dell'articolo 3 del regolamento (UE) 2015/2120, che stabilisce misure riguardanti l'accesso a Internet aperto, e il regolamento (UE) n. 531/2012 relativo al *roaming* sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione.

Con la sentenza qui riportata, la Corte di giustizia dell'Unione Europea evidenzia che l'art. 3 del regolamento (UE) 2015/2120 sancisce il principio di neutralità di *Internet*, in ragione del quale i fornitori di servizi di accesso a *Internet* devono trattare tutto il traffico in modo uguale e senza discriminazioni, restrizione o interferenza, indipendentemente dalle applicazioni o dai servizi utilizzati. Sono possibili sono misure ragionevoli di restrizione del traffico, che per essere tali devono però essere trasparenti, non discriminatorie e proporzionate, non basate su considerazioni commerciali, ma su differenze tecniche oggettive tra alcune categorie di traffico, non riguardare monitoraggio dei contenuti e non essere mantenuto più a lungo del necessario. Il co. 3 dell'art. 3 prevede inoltre che i fornitori di servizi di accesso a *Internet* non possano applicare misure di gestione del traffico che vadano oltre quelle sopra indicate e, in ogni caso devono astenersi dal bloccare, rallentare, modificare, limitare, interrompere, degradare o discriminare specifiche applicazioni, categorie di applicazioni, servizi o categorie di servizi se non per motivi tecnici, non su considerazioni di ordine commerciale.

Inoltre, il Considerando 7 del regolamento 2015/2120 prevede che fornitore e utente possano concludere degli accordi sulle condizioni e sulle caratteristiche commerciali e tecniche dei servizi di accesso a *Internet* che il

primo deve fornire al secondo, come il prezzo da pagare e il volume di dati nonché la velocità corrispondenti, che però non devono limitare l'esercizio dei diritti degli utenti finali né permettere di eludere le disposizioni di detto regolamento che proteggono l'accesso a un'Internet aperta. Diverse sono, invece, le pratiche commerciali di cui all'articolo 3, paragrafo 2, del regolamento 2015/2120, adottate dai fornitori di servizi di accesso a *Internet* e che, contrariamente dagli accordi, non si traducono un incontro di volontà tra tale fornitore e un utente finale. Tali pratiche commerciali possono includere la condotta di un fornitore di servizi di accesso a Internet consistente nel proporre varianti o combinazioni specifiche di tali servizi ai suoi potenziali clienti, al fine di rispondere alle aspettative e alle preferenze di ognuno di essi, e, se del caso, di concludere con ciascuno di essi un accordo individuale. In ogni caso, però, al pari degli accordi, tali pratiche commerciali non devono limitare l'esercizio dei diritti degli utenti finali, né permettere di eludere le disposizioni di tale regolamento che proteggono l'accesso a un'*Internet* aperta.

Pertanto, la Corte ha ritenuto che i pacchetti in questione, in quanto contenenti accordi mediante i quali una volta esaurito il volume di dati compresi nel piano tariffario acquistato consentono ai sottoscrittori un accesso senza restrizioni solo a talune applicazioni e a taluni servizi soggetti a «tariffa zero», comportino una limitazione all'esercizio dei diritti di cui all'articolo 3, paragrafo 1, del regolamento 2015/2120, trattandosi di limitazione al traffico non ragionevole perché basata su motivi di ordine commerciale.

Corte di Giustizia UE, Grande Sezione, sentenza 15 settembre 2020, cause riunite C-807/18 e 39/19

3. Pubblicata la XXXIa relazione annuale della Commissione Europea al Parlamento e al Consiglio sulla tutela degli interessi finanziari dell'Unione europea e sulla lotta contro la frode

In data 3 settembre 2020 è stata pubblicata la Trentunesima relazione annuale sulla tutela degli interessi finanziari dell'Unione europea e sulla lotta contro la frode, relativa all'anno 2019 a cura della Commissione europea. Con particolare riferimento all'utilizzo degli strumenti informatico per il contrasto alle frodi, la relazione effettua dapprima una ricognizione degli strumenti legislativi esistenti, ovvero il regolamento (CE) n. 515/97 sulla mutua assistenza amministrativa in materia doganale, che definisce le modalità di cooperazione tra gli organi amministrativi degli Stati membri e tra essi e la Commissione europea nella lotta alle frodi doganali, in particolare sullo scambio reciproco di informazioni. Nella relazione la Commissione evidenzia che di tale regolamento è stato avviato nel 2019 un processo di valutazione. Tale regolamento è poi stato modificato dal regolamento (UE) 2015/1525, che ha introdotto altre due banche dati, ossia il repertorio dei messaggi sullo status dei container (CSM, Container Status Messages) e il repertorio importazioni, esportazioni e transito (IET) e che fa progredire il quadro di cooperazione accelerando le indagini dell'OLAF e facilitando l'uso delle informazioni ottenute sulla base dell'assistenza reciproca come prove nei procedimenti giudiziari nazionali.

La Commissione descrive poi il Sistema d'informazione antifrode (Anti-Fraud Information System, AFIS), ovvero una serie di applicazioni informatiche antifrode gestite dalla Commissione europea destinate a consentire lo scambio tempestivo e sicuro di informazioni relative alle frodi tra le amministrazioni competenti nazionali e dell'UE, nonché la conservazione e l'analisi di dati pertinenti. Inoltre, riporta le Operazioni doganali congiunte (ODC) coordinate o sostenute dall'OLAF nel 2019, che oltre a fornire ai paesi coinvolti il sostegno necessario per l'esecuzione di azioni coordinate attraverso la sua infrastruttura tecnica permanente e i suoi strumenti informatici e di comunicazione, ha messo a disposizione anche analisi strategiche e un sostegno amministrativo e finanziario.

Con riguardo ai criteri relativi ai rischi finanziari, la Commissione dà atto di aver adottato nel maggio 2018 la decisione di esecuzione n. C (2018) 3293, che stabilisce misure per l'applicazione uniforme dei controlli doganali stabilendo criteri e norme comuni in materia di rischi finanziari. Poco più avanti descrive il funzionamento del sistema comune doganale di gestione dei rischi (CRMS), concepito per mettere a disposizione un meccanismo rapido e di facile utilizzo per lo scambio diretto di informazioni relative ai rischi tra funzionari operativi e centri di analisi dei rischi negli Stati membri. Di esso fa parte il modulo d'informazione sul rischio (RIF), che viene compilato *online* e messo immediatamente a disposizione di tutti gli uffici doganali collegati e garantisce che le informazioni sui rischi nuovi e significativi individuati siano distribuite il più rapidamente possibile agli uffici doganali operativi in tutti gli Stati membri.

La Commissione descrive poi i diversi progetti esistenti per consentire un approccio europeo integrato volto a rafforzare la gestione dei rischi doganali e sostenere controlli efficaci da parte degli Stati membri. In

particolare, il progetto INTELF4CUSTAF, istituito nel 2018 dall'OLAF con la collaborazione del Centro comune di ricerca, e i cinque progetti pilota introdotti nel 2019, che hanno riunito esperti degli Stati membri interessati con l'obiettivo di condividere esperienze e analisi di prova, alcuni dei quali hanno sviluppato approcci nuovi e più sperimentali quali un tentativo di rilevare sistematicamente gli operatori elettronici (eTraders) utilizzando dichiarazioni DAU (documento amministrativo unico) oppure un nuovo approccio volto a individuare container potenzialmente sospetti in base al peso. Un ulteriore progetto pilota sulla capacità di analisi congiunta destinato ad analizzare i dati sui flussi commerciali è stato attuato nel 2019 l'OLAF e dei servizi della Commissione interessati: l'analisi ha individuato rischi elevati di dichiarazione errata per diversi prodotti oggetto di misure di difesa commerciale che meritavano un seguito a livello operativo, quale la diffusione di informazioni sui rischi agli Stati membri (RIF).

Per quanto riguarda le iniziative assunte dai singoli Stati membri, nel settore delle frodi doganali Gli Stati membri hanno segnalato otto misure. Tre hanno natura operativa, quali la condivisione delle migliori prassi nel settore dei controlli successivi allo sdoganamento tra i paesi del gruppo di Visegrad, l'introduzione di una gestione dei rischi basata sulle persone fisiche e sui prodotti e l'introduzione di un sistema di profilazione e segmentazione degli operatori economici. Due Stati membri hanno comunicato una misura organizzativa, ad esempio la circolare "Fascicoli OLAF sulle risorse proprie tradizionali (RPT)" o l'istituzione di una direzione di pianificazione e coordinamento operativi. Altri due Stati membri hanno comunicato misure amministrative, segnatamente il rilevamento di merci dichiarate in modo falso e misure nel settore delle entrate fiscali. Nel settore delle frodi fiscali, invece, gli Stati membri hanno comunicato cinque misure. Tre di esse hanno natura operativa: la Croazia ha riferito di aver organizzato attività di formazione tecnica sugli "strumenti per il monitoraggio e l'audit del commercio elettronico e l'acquisizione di strumenti", l'Estonia ha aumentato le ispezioni dei subappaltatori nel settore delle costruzioni, mentre l'Italia ha introdotto applicazioni informatiche per contrastare le frodi in materia di IVA. La Polonia ha inoltre segnalato due misure legislative nel settore delle frodi fiscali riguardanti tra l'altro modifiche della legge in materia di IVA.

Infine, la Commissione evidenzia che tanto per le irregolarità fraudolente quanto per quelle non fraudolente, si è registrata una diminuzione del numero di casi segnalati rispetto alla media quinquennale, accompagnata tuttavia da un aumento degli importi corrispondenti.

Trentunesima relazione annuale sulla tutela degli interessi finanziari dell'Unione europea e sulla lotta contro la frode (2019)

4. Deroghe alla direttiva *e-privacy* per la lotta contro gli abusi sessuali sui minori *online*

Constato che alcuni fornitori di servizi di comunicazione interpersonale indipendenti dal numero (quali i servizi di messaggistica e di posta elettronica basati sul *web* nonché la telefonia via Internet) stanno già utilizzando tecnologie specifiche per individuare gli abusi sessuali sui minori nell'ambito dei loro servizi e segnalarli alle autorità di contrasto e alle organizzazioni pubbliche contro gli abusi sessuali sui minori e/o per rimuovere il materiale pedopornografico, la Commissione europea ha avanzato una Proposta di Regolamento europeo che prevede una deroga temporanea a talune disposizioni della direttiva 2002/58/CE, c.d. direttiva *e-privacy*, che tutela la riservatezza delle comunicazioni e dei dati sul traffico. Con tale regolamento la Commissione propone di stabilire norme temporanee e rigorosamente limitate che derogano agli obblighi specifici di cui all'articolo 5, paragrafo 1, e all'articolo 6 direttiva 2002/58/CE, i quali non si applicherebbero, a certe condizioni, al trattamento dei dati personali e di altro tipo connesso alla fornitura di servizi di comunicazione interpersonale indipendenti dal numero strettamente necessario per l'uso della tecnologia al solo scopo di rimuovere materiale pedopornografico e di individuare o segnalare gli abusi sessuali sui minori *online* alle autorità competenti. Il Regolamento si applicherebbe dal 21 dicembre 2020 fino al 31 dicembre 2025.

Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE, COM(2020) 568 final

5. Linee guida dell'*European Data Protection Board* sull'interpretazione di alcuni aspetti della disciplina europea in materia di protezione dei dati personali

Sono state adottate e aggiornate le linee guida dell'*European Data Protection Board* sull'interpretazione di alcuni aspetti della normativa europea in materia di protezione dei dati personali. Il 7 luglio 2020 sono state aggiornate le linee guida sulla disciplina relativa al diritto alla cancellazione di cui all'art. 17 del Regolamento europeo per la protezione dei dati personali 679/2016 (GDPR), con riguardo alle sole richieste avanzate verso i motori di ricerca *online*. In particolare, le linee guida si occupano di fornire indicazioni su: (i) i motivi (cumulabili tra loro) per cui l'interessato può avanzare una richiesta di cancellazione dei propri dati personali ad un motore di ricerca, elencati all'art. 17 § 1 GDPR; (ii) le eccezioni che il motore di ricerca può opporre all'interessato che formula richiesta di cancellazione, elencate all'art. 17 § 3 GDPR.

Il 2 settembre 2020 sono state invece adottate le linee guida che specificano i concetti, per come definiti all'art. 4 del GDPR, di: (i) titolare (*controller*) del trattamento, normalmente un'organizzazione, ma può trattarsi anche di una persona fisica, che decide determinati elementi chiave, come le finalità e i mezzi, del trattamento dei dati, riconosciuto come tale dalla legge o sulla base di un'analisi degli elementi di fatto o delle circostanze del caso; (ii) contitolari (*joint controller*) del trattamento, figura disciplinata all'art. 26 del GDPR e che riguarda il caso in cui più entità collaborino nella determinazione dei fini e dei mezzi del trattamento, il quale non sarebbe possibile senza la partecipazione di entrambe le parti; (iii) responsabile (*processor*) del trattamento, soggetto che tratta i dati personali per conto e secondo le indicazioni del titolare del trattamento; (iv) la relazione che sussiste tra i suddetti soggetti. Si tratta di concetti che delineano i ruoli cruciali su cui si articola la disciplina europea in materia di protezione dei dati personali.

Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)

Guidelines 07/2020 on the concepts of controller and processor in the GDPR

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Entrata in vigore riforma delle intercettazioni

Dal 1° settembre 2020 è entrata in vigore la nuova disciplina delle intercettazioni di cui al decreto legislativo 29 dicembre 2017, n. 216, come modificato dal decreto-legge 30 dicembre 2019, n. 161, convertito con modificazioni dalla legge 28 febbraio 2020, n. 7.

Ministero della Giustizia Circolare 31 agosto 2020 - Completamento della digitalizzazione e securizzazione delle intercettazioni, avvio della nuova disciplina dal 1 settembre

2. Convertito in legge il Decreto Semplificazioni

È stata pubblicata nella Gazzetta Ufficiale del 14 settembre 2020, n.228 la legge 11 settembre 2020, n. 120 di conversione, con modificazioni, del decreto-legge 16 luglio 2020, n. 76 recante «misure urgenti per la semplificazione e l'innovazione digitale». Le modifiche apportate dal d.l. in oggetto al d.lgs. 7 marzo 2005, n. 82, c.d. Codice dell'amministrazione digitale, sono state confermate, in particolare la semplificazione e il rafforzamento dell'accesso al domicilio digitale per i cittadini, specie per le persone con disabilità, nonché l'accesso a tutti i servizi digitali della Pubblica amministrazione tramite SPID, Carta d'identità elettronica (CIE) e tramite AppIO su smartphone. Tra le novità confermate vi è l'istituzione del c.d. domicilio digitale per i professionisti, anche non iscritti in albi, accompagnato dalla sanzione della sospensione dall'albo per il professionista che non comunica il proprio indirizzo PEC all'Ordine di appartenenza e la statuizione che la verifica dell'identità digitale con livello di garanzia almeno significativo, ai sensi dell'articolo 8, paragrafo 2, del Regolamento (UE) n. 910/2014 del 23 luglio 2014, produce, nelle transazioni elettroniche o per l'accesso ai servizi in rete, gli effetti del documento di riconoscimento equipollente.

È stata poi confermata la disposizione di cui all'art. 26, col quale è stata istituita la piattaforma per la notificazione digitale degli atti della pubblica amministrazione, alla quale si accede tramite SPID o Carta d'identità elettronica, e si prevede che ai fini della notificazione di atti, provvedimenti, avvisi e

comunicazioni, in alternativa alle modalità previste da altre disposizioni di legge, anche in materia tributaria, le amministrazioni possono rendere disponibili telematicamente sulla piattaforma i corrispondenti documenti informatici. Inoltre, è stato confermato che tale modalità di notificazione per il momento non si applica agli atti del processo civile, penale, per l'applicazione di misure di prevenzione, amministrativo, tributario e contabile e ai provvedimenti e alle comunicazioni ad essi connessi, agli atti della procedura di espropriazione in materia di riscossione delle imposte sul reddito indicati e atti dei procedimenti di competenza delle autorità provinciali di pubblica sicurezza relativi a pubbliche manifestazioni, misure di prevenzione personali e patrimoniali, autorizzazioni e altri provvedimenti a contenuto abilitativo, soggiorno, espulsione e allontanamento dal territorio nazionale degli stranieri e dei cittadini dell'Unione europea, a carattere preventivo in materia di pubblica sicurezza, e ai provvedimenti e alle comunicazioni ad essi connessi. Per questi ultimi è stato aggiunto l'inciso «*o comunque agli atti di ogni altro procedimento*».

È poi rimasto invariato anche l'art. 28, che si occupa della semplificazione della notificazione e comunicazione telematica degli atti in materia civile, penale, amministrativa, contabile e stragiudiziale e dispone che le amministrazioni pubbliche possono comunicare gli indirizzi di posta elettronica certificata di propri organi o articolazioni, anche territoriali, presso cui eseguire le comunicazioni o notificazioni per via telematica nel caso in cui sia stabilito presso questi l'obbligo di notifica degli atti introduttivi di giudizio in relazione a specifiche materie ovvero in caso di autonoma capacità o legittimazione processuale.

La legge di conversione ha poi introdotto un inedito art. 27-bis, che aggiunge un nuovo co. 7-bis all'art. 55 del d.lgs. 1° agosto 2003, n. 259, c.d. codice delle comunicazioni elettroniche, e che prevede la semplificazione dell'obbligo di identificazione previsto dal co. 7 dell'art. 55 cit. in caso di acquisto di schede elettroniche (S.I.M.) utilizzate per la fornitura di servizi di tipo "internet delle cose", installate senza possibilità di essere estratte all'interno degli oggetti connessi e che, anche se disinstallate, non possono essere utilizzate per effettuare traffico vocale, inviare SMS o fruire del servizio di connessione a internet.

Infine, è stato confermato anche l'art. 31, col quale erano state introdotte alcune disposizioni in materia di semplificazione dei sistemi informativi delle pubbliche amministrazioni e dell'attività di coordinamento nell'attuazione della strategia digitale e in materia di perimetro di sicurezza nazionale cibernetica, nonché l'art. 32, che ha istituito il Codice di condotta tecnologica, allo scopo di disciplinare le modalità di progettazione, sviluppo e implementazione dei progetti, sistemi e servizi digitali delle amministrazioni pubbliche, nel rispetto della disciplina in materia di perimetro nazionale di sicurezza cibernetica.

Testo coordinato del Decreto-legge 16 luglio 2020 n. 76, c.d. Decreto Semplificazioni

3. Il recepimento della Direttiva (UE) 2017/1371 (c.d. Direttiva PIF)

Con il D.lgs. n. 75 del 14 luglio 2020 l'ordinamento italiano recepisce la Direttiva 1371/2017, c.d. Direttiva PIF, recante norme per la "lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale". Il Decreto Legislativo modifica alcune norme del codice penale, prevedendo, da una parte, inasprimenti di pena per i reati di cui agli artt. 316, 316 ter e 319 quater c.p., e, dall'altra parte, estendendo la portata applicativa delle fattispecie di cui all'art. 322 bis c.p., attraverso l'inserimento del comma 5 *quinquies* al primo comma della disposizione, e all'art. 640 comma 2, n. 1) c.p., mediante l'equiparazione dell'Unione Europea allo Stato e agli altri enti pubblici quali persone offese del reato.
Si segnalano infine le principali modifiche apportate al D.lgs. n. 231/2001: (i) all'art. 24 sono state introdotte le fattispecie di frode nelle pubbliche forniture di cui all'art. 356 c.p. ed il reato di frode in agricoltura di cui all'art. 2 della L. n. 898/1986; (ii) la responsabilità degli enti per i reati di cui all'art. 25 viene estesa anche per i fatti che offendono gli interessi finanziari dell'Unione Europea; (iii) viene aggiunto il comma 1 *bis* all'art. 25 *quinquiesdecies,* che prevede, in relazione alla commissione dei reati tributari previsti dal d.lgs. n. 74/2000, se «*commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro*», l'irrogazione della sanzione pecuniaria fino a trecento quote per il delitto di dichiarazione infedele e fino a quattrocento quote per i delitti di omessa dichiarazione e indebita compensazione.

Per approfondire: MAZZANTI E., *La riforma delle frodi europee in materia di spese. Osservazioni a prima lettura sull'attuazione della 'direttiva pif' (d.lgs. 14 luglio 2020, n. 75)*, in *Sistema Penale,* 23 settembre 2020; CORSARO C., ZAMBRINI M., *Il recepimento della Direttiva PIF e le novità in materia di reati contro la*

pubblica amministrazione e reati tributari. L'ulteriore ampliamento dei reati presupposto per la responsabilità degli enti, in *Giurisprudenza Penale*, 21 luglio 2020.

Decreto Legislativo 14 luglio 2020, n. 75

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. *Sexting* e violenza sessuale nei confronti di minori

La Suprema corte ha ritenuto che la condotta di colui che, dopo aver inviato ad una ragazza minorenne una serie di messaggi di *whatsapp* allusivi e sessualmente espliciti, l'ha costretta a inviargli a sua volta una foto senza reggiseno nonché a commentare la foto da lei ricevuta ritraente il membro maschile, minacciandola altrimenti di pubblicare la *chat* su *instagram* e su pagine *hot*, integri il reato di violenza sessuale aggravata di cui agli artt. 609-*bis* e 609-*ter* c.p. In particolare, ha sostenuto che nella violenza sessuale non rileva la mancanza di contatto fisico tra vittima e reo, poiché tale reato può essere commesso anche mediante strumenti telematici di comunicazione a distanza, e che tale condotta è oggettivamente idonea a violare la libertà di autodeterminazione sessuale della vittima, poiché coinvolge indirettamente la sua corporeità.

Conformi: Corte di Cassazione, sez. III Penale, sentenza 24 aprile 2019 (ud. 30 ottobre 2018), n. 17509/2018 – Pres. Giulio Sarno, Rel. Aldo Aceto; Corte di Cassazione, sez. III penale, sentenza 12 giugno 2013 (ud. 9 maggio 2013), n. 25822/2013 - Pres. Claudia Squassoni, Rel. Santi Gazzara.

Per approfondire: SALVADORI I., *Sexting, minori e diritto penale*, in *Cybercrime*, a cura di A. Cadoppi, S. Canestrari, A. Manna e M. Papa, Torino, 2019, p. 567 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 M. Bertolino e G. Forti (cur.), *Scritti per Federico Stella*, Napoli 2007, vol. II, p. 1267 ss.

Corte di Cassazione, sez. III Penale, sentenza 8 settembre 2020 (ud. 2 luglio 2020), n. 25266/2020 - Pres. Elisabetta Rosi, Rel. Ubalda Macrì

2. Vendita di *bitcoin* e abusivismo finanziario

Anche le valute virtuali possono essere soggette alla normativa in materia di servizi finanziari nel caso in cui la vendita di *bitcoin* venga reclamizzata come una vera e propria proposta di investimento, con tanto di pubblicità su di un sito Internet contenente informazioni idonee a mettere i risparmiatori in grado di valutare se aderire o meno all'iniziativa. Pertanto, in tal caso si devono rispettare gli adempimenti prescritti in materia di servizi finanziari di cui agli artt. 91 ss. T.U.F., in mancanza dei quali sussiste il reato di abusivismo finanziario di cui all'art. 166, comma 1, lett. c) TUF.

Per approfondire: VADALÀ R.M., *Criptovalute e cyberlaundering: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, Sist. Pen., 2020; PICOTTI L., *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ.*, 2018, n. 3-4, p. 590 ss; PLANTAMURA V., *Il cybericiclaggio*, in *Cybercrime* a cura di A. Cadoppi, S. Canestrari, A. Manna e A. Papa, Torino, 2019, p. 859 ss.; CAPACCIOLI S., *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015; PICOTTI L. *Rilevanza penale degli obblighi di registrazione della clientela in ambito bancario nella normativa antiriciclaggio*, in *RGEA*, 2010, n. 8, p. 163; STURZO, *Bitcoin e riciclaggio 2.0.*, in *Dir. pen. cont.*

Corte di Cassazione, sez. II penale, sentenza 25 settembre 2020 (ud. 17 settembre 2020), n. 26807/2020 - Pres. Domenico Gallo, Rel. Giuseppe Coscioni

3. Accesso abusivo ad un sistema telematico oltre i limiti dell'autorizzazione e *overruling in malam partem*

Integra reato di accesso abusivo *ex* art. 615 *ter* c.p. la condotta di accesso e mantenimento ad un sistema telematico protetto commessa da un soggetto autorizzato in violazione dei limiti e i fini connessi alla propria autorizzazione, anche se si tratta di condotta realizzata prima dell'arresto delle Sezioni Unite del 2017 (Cass. n. 41210 del 18/05/2017), che ha risolto in senso positivo il contrasto giurisprudenziale sorto in merito alla rilevanza penale di tale fattispecie, precisando la direzione esegetica assunta già dalle stesse Sezioni Unite in una precedente sentenza del 2011 (Cass. n. 4694 del 27/10/2011), non introducendo, peraltro, alcuna innovazione giurisprudenziale eccentrica rispetto alle precedenti riflessioni svolte anche nell'ambito delle Sezioni semplici.

La Suprema Corte, uniformandosi alla giurisprudenza sul punto (cfr. da ultimo Cass. sez. un. n. 8544 del 24/19/2019), conferma infatti che non vi è *overruling* in contrasto con l'art. 7 CEDU quando l'interpretazione colpevolista sia già emersa precedentemente alla commissione del fatto nell'ambito della giurisprudenza di legittimità.

Conformi: Corte di Cassazione, sez. V penale, sentenza 6 agosto 2018 (ud. 24 aprile 2018), n. 37857/2018 – Pres. Maria Vessichelli, Rel. Rosa Pezzullo.

Per approfondire: FLOR R., *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in *Cybercrime* a cura di A. Cadoppi, S. Canestrari, A. Manna e A. Papa, Torino, 2019, p. 142 ss.; SALVADORI I., *I reati contro la riservatezza informatica*, in *Cybercrime* a cura di A. Cadoppi, S. Canestrari, A. Manna e M. Papa, Torino, 2019, p. 656 ss.; FLOR R., *La condotta del pubblico ufficiale fra violazione della voluntas domini, "abuso" dei profili autorizzativi e "sviamentodi poteri"*, in *Dir. Pen. Proc.*, 2018, n. 4, p. 506 ss.; FLOR R., *Verso una rivalutazione dell'art. 615-ter c.p.?* in *Riv. Trim. Dir. Pen. Cont.*, 2011, p. 126 ss.; SALVADORI I., *Quando un insider accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615-ter c.p.*, in *Riv. Trim. Dir. Pen. Economia*, 2012, 369 ss.; SALVADORI I., *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in L. Picotti (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 125 ss.; PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004.

Corte di Cassazione, sezione V penale, sentenza 11 settembre 2020 (ud. 9 luglio 2020), n. 25944/2020 - Pres. Maria Vessichelli, Rel. Paola Borrelli

4. Il concorso tra i reati di frode informatica e di sostituzione di persona

La Suprema Corte evidenzia che, prima dell'introduzione della nuova fattispecie aggravata di cui al co. 3 dell'art. 640 ter c.p., che punisce la frode informatica commessa con furto o indebito utilizzo dell'identità digitale, la condotta di intervento senza diritto sul sistema informatico e telematico protetto da *password* di un servizio di *home banking* e l'assunzione di falsa identità del titolare di una carta banco posta tramite l'utilizzo di codici personali identificativi integrava non solo il reato di frode informatica, ma anche quello di sostituzione di persona ex art. 494 c.p., essendo idonea ad ingannare persone fisiche che ripongono affidamento in sistemi informatici garantiti da misure di sicurezza. Dunque, il delitto di frode informatica ex art. 640-ter c.p. e quello di sostituzione di persona di cui all'art. 494 c.p. potevano concorrere tra loro.

Conformi: Corte di Cassazione, sez. II penale, sentenza 24 settembre 2018 (ud. 26 giugno 2018), n. 41013/2018 – Pres. Antonio Prestipino, Rel. Marco Monaco

Per approfondire: MINICUCCI G., *Le frodi informatiche*, in *Cybercrime* a cura di A. Cadoppi, S. Canestrari, A. Manna e M. Papa, Torino, 2019, p. 827 ss; CAJANI F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni nella l. 15 ottobre 2013, n. 119)*, in *Cass. pen.*, 2014, 1094 ss.; CIPOLLA P., *Social network, furto di identità e reati contro il patrimonio*, in *Giur. merito*, 2012, n. 12, p. 2672 ss; FLOR R., *phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, n. 2-3, p. 899 ss.; PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004.

Corte di Cassazione, sez. II penale, sentenza 11 agosto 2020 (ud. 2 luglio 2020), n. 23760/2020 – Pres. Domenico Gallo, Rel. Alfredo Mantovano

CONTRIBUTI DOTTRINALI DI RILIEVO

Diritto di Internet 2020

L. PICOTTI, *La violenza sessuale via Whatsapp*, in corso di pubblicazione

C. CRESCIOLI, *Profili penali della creazione di un falso profilo Facebook a scopo diffamatorio*, in corso di pubblicazione

Sistema Penale

D. ALBANESE, *Caso Palamara: il g.i.p. di Perugia ritiene "casuali" le intercettazioni nei confronti dei parlamentari e dispone l'acquisizione delle conversazioni*

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