News luglio e agosto 2021

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

NOVITÀ SOVRANAZIONALI

1. La deroga temporanea alla direttiva 2002/58/CE sulla riservatezza per consentire l'individuazione degli abusi sessuali *online* sui minori

Il regolamento UE ha previsto norme temporanee e rigorosamente limitate che derogano a determinati obblighi previsti dalla direttiva 2002/58/CE, direttiva relativa alla vita privata e alle comunicazioni elettroniche, al solo scopo di consentire ai fornitori di alcuni servizi di comunicazione interpersonale indipendenti dal numero di utilizzare tecnologie specifiche per il trattamento di dati personali e di altro tipo nella misura strettamente necessaria a individuare gli abusi sessuali *online* sui minori sui propri servizi e segnalarli e a rimuovere il materiale pedopornografico *online* dai loro servizi. In particolare, il regolamento prevede la sospensione del divieto di ascolto, captazione, memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni e dei relativi dati sul traffico, divieto di cui all'art. 5 par. 1 della direttiva 2002/58/CE, nonché dell'obbligo di cancellare o anonimizzare i dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica, di cui all'art. 6 part. 1 della direttiva 2002/58/CE. Tale deroga opera solo qualora il trattamento dei dati personali sia strettamente necessario per l'uso della tecnologia specifica al solo scopo di individuare e rimuovere materiale pedopornografico *online* e di segnalarlo alle autorità di contrasto e alle organizzazioni che agiscono nell'interesse pubblico contro gli abusi sessuali sui minori, nonché di individuare l'adescamento di minori e segnalarlo alle autorità di contrasto o alle organizzazioni che agiscono nell'interesse pubblico contro gli abusi sessuali sui minori. Qualora venga individuato un presunto abuso sessuale *online* a danno di minori, i fornitori devono conservare in modo sicuro i dati sul contenuto e i relativi dati sul traffico, unicamente per segnalare senza indugio il presunto abuso sessuale online sui minori alle competenti autorità di contrasto e giudiziarie o alle organizzazioni che agiscono nell'interesse pubblico contro l'abuso sessuale sui minori. Inoltre devono bloccare il conto dell'utente interessato o sospendere o porre fine al servizio offertogli, ma devono altresì consentire all'utente interessato di presentare ricorso presso il fornitore o di chiedere l'avvio di un riesame amministrativo o di proporre ricorsi giurisdizionali su questioni relative al presunto abuso sessuale online sui minori e devono rispondere, in conformità del diritto applicabile, alle richieste di fornire i dati necessari per la prevenzione, l'accertamento, l'indagine o il perseguimento di reati di cui alla direttiva 2011/93/UE, provenienti delle autorità giudiziarie e di contrasto competenti.

Regolamento (UE) del Parlamento Europeo e del Consiglio del 14 luglio 2021 n. 1232 relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE

2. L'*European Data Protection Board* si esprime sul progetto della BCE dell'"euro digitale"

L'*European Data Protection Board* (EDPB) ha espresso la propria opinione in relazione al report sull'euro digitale elaborato dalla Banca Centrale Europea (BCE) nell'ottobre 2020, inviando una lettera alle diverse istituzioni europee coinvolte. La BCE ha infatti iniziato un'opera di consultazione degli *stakeholders* e del pubblico sul suo progetto di creare una valuta digitale nella zona Euro ("*digital euro*") per renderla disponibile con riguardo ai pagamenti del commercio al dettaglio quale alternativa alla moneta fisica.
Tale progetto solleva diverse questioni in tema di privacy e protezione dei dati personali. Tra questi l' EDPB evidenzia come l'uniformarsi ad un alto standard sia cruciale per rinforzare la fiducia degli utenti verso l'utilizzo di un "euro digitale", traducendo il rispetto della protezione dei dati personali già nel corso delle preliminari fasi e misure di progettazione e programmazione, secondo i dettami del principio della *data protection by design* e *by default.*
I maggiori rischi che l'iniziativa per un "euro digitale" presenta riguardano la potenziale tracciabilità delle transazioni degli utenti effettuate attraverso tale sistema di pagamento. A questo riguardo l' EDPB formula diversi suggerimenti, tra questi la preferibilità di un approccio decentralizzato fondato sull'utilizzo di token

(*token-based, decentralised approach*) e l'opportunità di offrire una modalità di transazioni offline effettuabili anonimamente o, quantomeno, con un alto livello di pseudonimizzazione.

EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro

3. Pacchetto proposte Commissione per il contrasto del riciclaggio e del finanziamento del terrorismo (cd. AML/CFT)

In data 20 luglio 2021 la Commissione ha proposto un pacchetto d'interventi legislativi per il miglioramento del sistema antiriciclaggio al fine di agevolare l'individuazione delle operazioni e delle attività sospette e sanare le lacune che sono sfruttate dai criminali.

Il pacchetto, con l'obiettivo esplicito di attuare gli impegni assunti con il piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo, adottato dalla Commissione il 7 maggio 2020, si compone delle seguenti quattro proposte di atti normativi, differenti per forma e contenuto:

1. Una proposta di regolamento che istituisce una nuova autorità dell'UE in materia di AML/CFT: Sono previste disposizione per l'istituzione di una nuova autorità antiriciclaggio sovranazionale (cd. *Authority for Anti-Money Laundering and Countering the Financing of Terrorism* o AMLA) quale centrale di coordinamento delle autorità nazionali. La proposta, nel regolamentarne composizione e poteri, affida, in particolare, all'AMLA: a. l'istituzione di un unico sistema integrato di vigilanza AML/CFT con metodologie uniche di valutazione del rischio e standard elevati, nonché il controllo e la gestione del c.d. AML/CFT *database*; b. il monitoraggio e il coordinamento degli organismi di vigilanza nazionali; c. la supervisione diretta - con poteri di indagine e sanzionatori particolarmente invasivi - di alcuni selezionati enti finanziari, identificati sulla base di appositi criteri, quali il carattere transfrontaliero ovvero l'esposizione elevata a determinati fattori di rischio; d. il miglioramento del coordinamento e della cooperazione tra le Unità di informazione finanziaria nazionali (c.d. FIU), mediante, anche, messa a disposizione, attraverso l'hosting FIU.net, di servizi e strumenti informatici e di intelligenza artificiale.
2. Una proposta di regolamento in materia di AML/CFT: La scelta operata con la proposta di usare un regolamento nasce dall'esigenza di garantire un maggiore livello di uniformazione nell'applicazione della disciplina antiriciclaggio nei vari Stati membri, prevedendo norme direttamente applicabili in tema di adeguata verifica e segnalazioni di operazioni sospette, nonché in termini di definizione delle nozioni di "titolare effettivo" o di "*persone politicamente esposte*" (c.d. PEP) o ancora di "*paesi terzi*". Quando l'iter legislativo sarà completato, verranno introdotte modifiche sostanziali a partire dell'elenco stesso dei soggetti obbligati alla disciplina antiriciclaggio, con riferimento soprattutto agli operatori di servizi digitali, per cui è prevista l'inclusione di tutti i fornitori di servizi di *crowdfunding* e l'estensione della cerchia dei fornitori di servizi di criptovalute. In particolare, rispetto a questi ultimi la Commissione intende recepire in toto le indicazioni del Gruppo d'Azione Finanziaria (GAFI-FAFT), vietando, anche, i portafogli anonimi di cripto-attività. Si prevede, inoltre, l'adozione, quale soglia per i pagamenti in contanti, nelle sole transazioni commerciali, di 10.000 euro, e si fissano, al fine di raggiungere una maggiore coerenza con la disciplina sulla protezione dei dati personali posta dal Regolamento UE 2016/679 (c.d GDPR), norme più specifiche circa le modalità di gestione e i tempi di conservazione di alcuni dati particolarmente sensibili acquisiti in sede di adeguata verifica, quali quelli previsti agli artt. 9 comma 1 e 10 del citato GDPR, includenti le informazioni relative a condanne penali riportate.
3. Una proposta di direttiva sui meccanismi che gli Stati membri devono mettere in atto per la prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che abroga la direttiva (UE) 2015/849: la Commissione intende dar avvio ad una riforma organica del quadro disciplinare ed istituzionale in conformità sia alla proposta di direttiva relativa all'istituzione di una nuova autorità di vigilanza di settore (c.d. AMLA vedi punto 1), sia a quella del regolamento sul contenuto degli obblighi antiriciclaggio (vedi supra punto 2). In particolare, con riguardo a questo

ultimo ambito la proposta ha una funzione integrativa-ampliativa, consentendo, anche, agli Stati membri di estendere le disposizioni del progetto di regolamento ad altri settori, con previsioni peculiari per i fornitori di servizi di gioco d'azzardo e dei fornitori di servizi di criptovalute. L'intervento intende anche implementare la coerenza complessiva operativa del sistema, prevendendo l'obbligo per la Commissione di condurre ogni 4 anni la valutazione dei rischi di riciclaggio e finanziamento del terrorismo (cd. AML/CFT) a livello dell'UE, basandosi sui pareri dell'AMLA, nonché sugli esiti delle valutazioni nazionali. All'AMLA compete la fissazione di linee guida e standard tecnici sulle condizioni per valutare e classificare i profili di rischio, nonché l'emanazione di norme tecniche di regolamentazione sulle condizioni generali per il funzionamento dei collegi di vigilanza AML/CFT su alcuni enti creditizi o finanziari transfrontalieri operanti in più Stati membri. Costituiscono novità le disposizioni relative all'operatività e alla vigilanza sugli organismi di autoregolamentazione, mentre sono una conferma del quadro esistente le previsioni sui requisiti di onorabilità degli alti dirigenti delle funzioni antiriciclaggio, relativamente alla ricorrenza, soprattutto, quale effetto ostativo, di precedenti penali. Ulteriori previsioni rilevanti attengono, poi, alla definizione dei potei e delle responsabilità delle FIU nazionali, nonché la cooperazione tra loro mediante la rete FIU.net e con le autorità nazionali. Sono regolamentati i casi di realizzazione di analisi congiunte da parte di più FIU e la delega all'AMLA dell'adozione di linee guida sui criteri per determinare quando una segnalazione di operazioni sospetta è di interesse per le FIU di altri Stati membri. Sul piano della cooperazione con le autorità nazionali è prevista l'istituzione di uno sportello unico dei registri dei conti bancari (c.d. RCB) che sarà sviluppato dalla Commissione e nel quale confluiranno le informazioni provenienti dai registri centralizzati dei conti bancari dei singoli Stati. La proposta contempla l'accesso a questo sportello soltanto da parte delle FIU, delegando ad un'apposita proposta di direttiva ad emendamento della direttiva (UE) 2019/1153, che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati, l'individuazione delle autorità nazionali legittimati all'accesso e dei casi in cui possono farlo. E' previsto che sia affidato sempre alla Commissione in tema di titolarità effettiva l'emanazione di un modello armonizzato per la notifica delle informazioni ai registri nazionali. Completano il quadro prospettato gli obblighi sanzionatori in capo agli Stati membri per violazione della disciplina antiriciclaggio: pur muovendosi nel solco dei precedenti interventi, le norme della proposta prevedono un certo livello di dettaglio e completezza, fissando anche una previsione apposita sulla tutela degli informatori o *Whistleblower*. Si tratta di una disposizione che individua i requisiti della tutela che gli Stati devono loro garantire, nonché i criteri procedurali e le forme di protezione che devono essere assicurati nel procedimento di segnalazione. Sul piano della natura delle sanzioni irrogabili, viene ribadita la preferenza per la natura amministrativa, con salvezza della facoltà dei singoli Stati membri di prevedere sanzioni penali e obbligo di comunicazione all'autorità giudiziaria competente nel caso in cui la violazione comporti anche la commissione di reati. Sul piano della tipologia delle sanzioni applicabili, ferma la previsione dei criteri sulla base dei quali valutare la gravità della violazione, ne sono individuate alcune con previsione in generale dell'obbligo della pubblicazione delle sanzioni irrogate e di comunicazione dell'irrogazione ed in generale dell'esito del procedimento sanzionatorio all'AMLA, che farà, anche, da tramite in proposito per lo scambio d'informazioni con le autorità di vigilanza degli altri Stati membri. Solo per le violazioni gravi e ripetute, attinenti ad alcuni aspetti espressamente indicati della disciplina antiriciclaggio, tra cui, ad esempio, l'adeguata verifica della clientela, la sanzione indicata è espressamente contemplata sia nella tipologia che nella misura, stabilendo la proposta quella pecuniaria pari nel massimo a due volte il beneficio tratto dalla violazione, laddove determinabile, ovvero ad almeno un milione di euro. E' altresì stabilito che questo importo sia ulteriormente aumentato per alcune tipologie di soggetti, consentendo in ogni caso agli Stati membri di autorizzare le autorità di vigilanza ad imporre sanzioni ancora superiori.

4. Una proposta di revisione del regolamento UE/2015/847 sui trasferimenti di fondi per il tracciamento dei trasferimenti di cripto-attività: In questo modo la Commissione intende conformarsi agli standard del GAFI e specificatamente alla Raccomandazione 15 relativa ai *virtual assets* ed ai relativi fornitori di servizi *(c.d. VASP)*. E' prevista, nello specifico, l'estensione della disciplina sui bonifici internazionali (c.d. '*travel rule'*) ai trasferimenti, anche in valuta *fiat*, effettuati dai '*crypto-assets*

services providers' (CASP), con oneri di tracciamento duplici, sia dell'ordinante che del beneficiario e previsione di forme di monitoraggio - in tempo reale ed ex post - a garanzia della completezza delle informazioni.

4. Revisione di 12 mesi degli standard del Gruppo d'Azione Finanziaria (GAFI-FAFT) sui virtual assets e sui fornitori di servizi relativi (cd. VASP)

In data 5 luglio 2021 il GAFI ha completato la revisione prevista dopo 12 mesi degli standard in oggetto, rilevando come ad oggi - sulla base dei dati relativi a 128 giurisdizioni - ancora 70 non si sono conformati, con conseguente assenza di un regime globale per prevenire l'uso per il riciclaggio di denaro o il finanziamento del terrorismo dei *virtual assets* e dell'operatività dei VASP. Il rapporto riporta anche dei dati relativi a transazioni *peer-to-peer*, riconoscendo come, nonostante il quadro non sia pienamente chiaro, si tratta certamente di una quota rilevante del mercato dei *virtual assets* e con una percentuale di commistione illecita certamente più alta rispetto alle transazioni mediante VASP. Alla luce di questi esiti, il GAFI intende proseguire le azioni di sostegno e monitoraggio sull'attuazione degli standard relativi a *virtual assets* e VASP, con un ulteriore verifica programmata per novembre 2021

Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs

5. Consultazione EBA su Linee guida sul ruolo, i compiti e le responsabilità della funzione compliance in materia di antiriciclaggio e contrasto al finanziamento del terrorismo

L'European Banking Authority (EBA) ha posto in pubblica consultazione, dal 29 luglio 2021 e fino al 2 novembre 2021 una proposta di Linee guida sul ruolo, i compiti e le responsabilità della funzione compliance in materia di contrasto al riciclaggio e al finanziamento del terrorismo (AML/CFT), da implementare proporzionalmente alla tipologia, alle dimensioni, alla natura, alla portata e alla complessità delle attività dell'operatore del settore finanziario, nonché ai rischi a cui è esposto. Obiettivo della proposta in consultazione è superare le differenze esistenti tra gli Stati Membri nell'implementazione della direttiva (UE) 2015/849 sulla governance AML/CFT degli operatori del settore finanziario, favorendo, in particolare, l'adozione di regole uniche e chiare sulla tempistica, il contenuto e la portata della procedura di segnalazione di operazioni sospette, quali presupposti di eventuali profili di responsabilità.

Consultation paper 29 luglio 2021

6. Parere della Banca centrale europea sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario.

In data 26 agosto 2021 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il parere del 4 giugno 2021 che la BCE ha emanato sulla proposta di regolamento in oggetto, manifestando il proprio favore per l'obiettivo - suo tramite perseguito - di eliminare gli ostacoli che si frappongono all'istituzione del mercato interno dei servizi finanziari e migliorarne il funzionamento, armonizzando le norme applicabili nel settore della gestione, della segnalazione e della verifica dei rischi relativi alle tecnologie dell'informazione e della comunicazione (TIC), nonché dei rischi relativi alle TIC derivanti da terzi. Tra le proposte avanzate per un migliore coordinamento dei contenuti della proposta con gli strumenti normativi esistenti si indica: 1. la definizione dell'esatto ambito di applicazione delle segnalazioni a cui una determinata entità finanziaria può essere soggetta ai sensi della proposta di regolamento e della proposta di direttiva NIS2; 2. l'introduzione di disposizioni apposite sul piano dei requisiti patrimoniali; 3. La previsione di un regime transitorio per gestire il periodo compreso tra l'entrata in vigore della proposta di regolamento e l'entrata in vigore delle norme tecniche di regolamentazione, in considerazione della circostanza che alcuni intermediari, compresi gli enti creditizi, sono già soggetti con riguardo a settori specifici a norme sui rischi relativi alle TIC più dettagliate rispetto alle disposizioni generali della proposta di regolamento; 4. l'allineamento di tutti i quadri di riferimento esistenti con riguardo alle definizioni, alle soglie e ai parametri relative alla segnalazione degli incidenti. Con

specifico riferimento, invece, al miglioramento delle disposizioni della proposta di regolamento, relative alla gestione dei rischi relativi alle TIC, ai test di resilienza operativa e ai rischi relativi alle TIC derivanti da terzi, tra le osservazioni avanzate dalla BCE si evidenzia: 1. l'introduzione sia di una definizione di «modifica di rilievo» in occasione della quale le entità finanziarie debbano effettuare la valutazione del rischio, sia di soglie quantitative dei costi e delle perdite rilevanti, da segnalare alle autorità competenti, causati dalle perturbazioni a livello di TIC e dagli incidenti connessi alle TIC; 2. la previsione nell'ambito della proposta di regolamento solo delle prescrizioni generiche in materia di test, con una descrizione più precisa nelle norme tecniche di regolamentazione e di attuazione; 3. ai fini della corretta classificazione dei fornitori terzi di servizi TIC critici, l'inserimento della consultazione della BCE previa adozione degli atti delegati che ne integrano i criteri.

Parere BCE 2021/C 343/01

7. Reports dei gestori delle piattaforme online sull'attività svolta nel mese di giugno nell'ambito del Programma di monitoraggio della disinformazione COVID-19

La Commissione ha pubblicato le relazioni di Facebook, Twitter, TikTok, Microsoft e Google sulle misure adottate a giugno per combattere la disinformazione sul coronavirus. Gli attuali firmatari e la Commissione stanno anche invitando nuove aziende ad aderire al codice di condotta sulla disinformazione, in quanto contribuirà ad ampliare il suo impatto e a renderlo più efficace.
Per esempio, su Twitter gli utenti possono ora addestrare sistemi automatici per identificare meglio le violazioni delle *policies* contro la disinformazione COVID-19 della piattaforma. Facebook ha collaborato con le autorità sanitarie internazionali per aumentare la consapevolezza pubblica sull'efficacia e la sicurezza dei vaccini e con i ricercatori della Michigan State University (MSU) per individuare e attribuire meglio i *deepfakes*. La prossima serie di rapporti sarà pubblicata a settembre. A seguito della recente pubblicazione (26 maggio 2021) da parte della Commissione degli orientamenti per rafforzare il codice di buone pratiche sulla disinformazione, i firmatari hanno dato il via al processo di rafforzamento del codice e hanno lanciato un invito congiunto a manifestare interesse per potenziali nuovi firmatari.

Per approfondire: GUERINI T., Fake news *e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Torino, 2020.

Reports dei gestori delle piattaforme nell'ambito della lotta alla disinformazione

9. Quinta riunione del Comitato *ad hoc* sull'Intelligenza Artificiale del Consiglio d'Europa

Il Comitato *ad hoc* sull'Intelligenza artificiale del Consiglio d'Europa (C*ouncil of Europe's Ad hoc Committee on Artificial Intelligence*, CAHAI) ha tenuto la sua quinta riunione plenaria online il 5-7 luglio 2021. In questa occasione il Comitato ha preso atto della relazione sui progressi compiuti e ha fornito orientamenti in merito alle questioni sollevate in tale documento. Tra i punti ritenuti rilevanti figurano la questione della natura dell'AI quale *dual-use technology*, potendo essere impiegata sia per svolgere attività lecite sia per perseguire finalità illecite. Evidenziando che gli aspetti militari non rientrano nelle competenze del Consiglio d'Europa, alcune delegazioni ritengono che la questione del *dual-use* debba essere completamente esclusa dagli elementi relativi al campo di applicazione di un eventuale strumento giuridicamente vincolante, a causa della difficoltà di distinguere tra l'uso civile e quello militare. Mentre altre delegazioni hanno sottolineato il valore aggiunto di affrontare le questioni relative agli usi non militari o civili delle applicazioni *dual-use* attraverso uno strumento giuridico.
Per quanto riguarda la classificazione dei rischi, tutte le delegazioni che si sono espresse hanno convenuto che dovrebbero essere formalizzati criteri chiari e comuni per la valutazione dell'impatto delle applicazioni d'AI, con un'enfasi sull'identificazione dei rischi per i diritti umani, la democrazia e lo stato di diritto. È stato anche notato che la valutazione dei rischi dovrebbe generalmente essere fatta in modo equilibrato, fornendo certezza e gradualità.
Infine, soffermandosi sugli aspetti relativi alla progettazione, sviluppo e ricerca dei sistemi di Intelligenza Artificiale, non vi è stata una chiara maggioranza tra le delegazioni che si sono espresse su come affrontare la regolamentazione delle fasi della ricerca dei sistemi di AI. Potrebbe quindi essere prudente non procedere con

uno strumento trasversale giuridicamente vincolante, ma si potrebbe ricorrere in futuro ad uno strumento (settoriale) giuridicamente non vincolante.

Per approfondire: SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista italiana di diritto e procedura penale*, 2021, n. 1, p. 83 ss.; ID., *Il diritto penale dei software a "duplice uso"*, in WENIN R., FORNSASARI G. (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali,* Napoli, 2017, p. 361 ss..

Meeting report and list of decisions, Council of Europe's Ad hoc Committee on Artificial Intelligence

10. Libertà di espressione e propaganda terroristica

E' lesiva della libertà d'espressione la condanna per propaganda terroristica ed incitamento alla violenza del ricorrente, il quale, nella sua qualità di imam, aveva condiviso nella sua pagina Facebook due immagini, postate da altri utenti del social network, relative rispettivamente ad un gruppo di uomini con armi ed uniformi, riferibili ad un gruppo considerato come terroristico in Turchia, e a dei manifestanti che avevano acceso un fuoco per strada, accompagnati dall'invito a condividerle per supportare le proteste che erano in corso al momento dei due post. Per la Corte Europea dei diritti dell'Uomo le decisioni nazionali di condanna, di primo e secondo grado, sono censurabili nella misura in cui non hanno valutato la condotta del ricorrente alla luce dei criteri fissati dalla giurisprudenza CEDU, non spiegando come i post in questione, alla luce del loro contenuto complessivo e del potenziale impatto sugli altri utenti di Facebook, fossero da considerare incitanti effettivamente alla violenza terroristica. In conseguenza di quanto sopra per la Corte i giudici nazionali non hanno realizzato quel legittimo bilanciamento tra le esigenze di prevenzione della criminalità e di tutela della sicurezza nazionale e il rispetto, che deve essere garantito in una società democratica, alla libertà di espressione.

Corte Europea dei diritti dell'Uomo, 31 agosto 2021, app. n. 23314/19 Üçdağ v. Turkey

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Pubblicata la conversione in legge del decreto-legge sulla *cybersecurity*

È stata pubblicata sulla Gazzetta Ufficiale n. 185 del 4 agosto 2021 la legge 4 agosto 2021, n. 109, di conversione in legge, con modificazioni, del d.l. 14 giugno 2021, n. 82, contenente disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. Con la legge di conversione è stata modificata leggermente la definizione di cybercicurezza ed è stata introdotta la definizione di resilienza nazionale nello spazio cibernetico, nei seguenti termini: "l*e attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma 1, lettera f), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131*". Altra novità è costituita dall'implementazione delle competenze della neocostituita Agenzia per la cybersicurezza nazionale, la quale, oltre a quelli già indicati nel decreto-legge, avrà anche il compito di assumere le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza e di provvedere alla qualificazione dei servizi *cloud* per la pubblica amministrazione. Inoltre, viene istituito, con funzioni di consulenza e di proposta, un Comitato tecnico-scientifico, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri.

Testo coordinato con la legge di conversione 4 agosto 2021, n. 109 del decreto-legge 14 giugno 2021, n. 82

2. Decreto del Presidente del Consiglio dei Ministri sulle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica

E' stato pubblicato nella Gazzetta Ufficiale n. 198 del 19 agosto 2021, il decreto del Presidente del Consiglio dei Ministri del 15 giugno 2021 che individua le categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105 (c.d. Decreto Cybersecurity), convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. A tal fine all'allegato 1 sono individuate quattro categorie generali con specificazione per ciascuna di esse dei beni, sistemi e servizi da impiegare nell'espletamento dei servizi informatici di cui all'art. 1, comma 2, lettera b), del decreto-legge e per cui vige l'obbligo dei soggetti inclusi nel perimetro e delle centrali di committenza che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT, di previa comunicazione del rischio associato all'oggetto della fornitura sia al Centro di valutazione e certificazione nazionale, sia ai centri di valutazione del Ministero dell'interno e del Ministero della difesa.

DPCM sulle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica

Per approfondire: PICOTTI L., VADALA' R.M., *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti,* in *Sistema Penale,* 5 marzo 2019; PICOTTI L., *Cybersecurity: quid novi?,* in *Diritto di Internet,* 2020, n. 1, p. 11 ss..

3. Schema del decreto legislativo di attuazione della direttiva attuazione della direttiva (UE) 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI

Il consiglio dei Ministri del 29 luglio 2021 ha approvato in esame preliminare e trasmesso alle Camere per l'acquisizione dei pareri del caso, lo schema del decreto legislativo di attuazione della direttiva (UE) 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI.
In evidente trasposizione della direttiva, lo schema del decreto reca le nozioni di strumento di pagamento diverso dai contanti, di record, di mezzo di scambio digitale e, quale sottocategoria di quest'ultimo, limitatamente alla funzione di pagamento, di valuta virtuale.
Sul piano degli interventi di natura spiccatamente penale, prevede, in particolare, la modifica della rubrica dell'art. 493-*ter* c.p. in "*indebito utilizzo e falsificazione di strumenti di pagamento diverso dai contanti*", conformemente alla sostituzione dell'oggetto materiale delle fattispecie contemplate da questo articolo con le leocuzioni: "*strumenti di pagamento immateriali, carte di credito o di pagamento, ovvero qualsiasi altro strumento o documento".* E', altresì, contemplata, al fine di riparametrare il regime sanzionatorio della frode informatica sulla falsariga di quello fissato dall'art. 493-*ter* c.p., l'introduzione- al secondo comma dell'art. 640-*ter* c.p.- della circostanza aggravante della produzione in conseguenza della stessa frode di un trasferimento di denaro, di valore monetario o di valuta virtuale. In ragione dell'obbligo d'incriminazione posto dall'art. 7 della direttiva, lo schema del decreto prevede, inoltre, il delitto, da contemplare in un nuovo art. 493-*quater* c.p., di detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti al fine di farne uso o di consentire ad altri di farne uso nella commissione di questi reati. Si tratta di un reato a dolo specifico avente ad oggetto dispositivi o programmi informatici per cui si richiede espressamente che siano materialmente progettati o specificatamente adattati al fine principale sopra indicato.
Per la menzionata fattispecie da emendare dell'art. 493-*ter* c.p., per quella aggravata di frode informatica e per quelle di nuovo conio di cui all'art. 493-*quater*, è stabilita, anche, la responsabilità amministrativa dipendente da reato delle persone giuridiche mediante introduzione nel d.lgs. 231/01 dell'art. 25-*octies*.1, che sarà rubricato "*illeciti in materia di mezzi di pagamento diversi dai contanti".*
L'art. 4 dello schema di decreto contempla, altresì, disposizioni apposite relative agli oneri di trasmissione da parte del Ministero della giustizia alla Commissione Europea d'informazioni sull'implementazione della direttiva e sui dati statistici inerenti i procedimenti penali e le indagini relativi agli strumenti di pagamento diversi dai contanti; mentre l'art. 5 definisce l'organo nazionale competente e la procedura da seguire per le richieste di scambio d'informazioni formulate dalle autorità degli stati membri sui reati relativi a questi strumenti.

Schema del decreto e relazione illustrativa

4. Schema del decreto legislativo di attuazione della direttiva (UE) 2019/1153 che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati, e che abroga la decisione quadro 2000/642/GAI

Sempre nel Consiglio dei Ministri del 29 luglio 2021 è stato approvato e trasmesso alle Camere per i pareri del caso il predetto schema di decreto, il quale si aggiunge a quanto già previsto sia dal d.lgs. 231/2001 sia dal d.lgs. 109/2007 ed individua nel procedimento penale ed in quello per l'applicazione delle misure di prevenzione patrimoniale le attività in relazione alle quali è possibile per alcune tipologie di reati l'accesso al registro centralizzato dei conti bancari e la richiesta di informazioni/ analisi finanziarie all'Unità d'informazione Finanziaria.
A tal fine l'art. 2 definisce, in particolare, le informazioni o analisi finanziarie, quali quelle detenute nella attività di prevenzione del riciclaggio e del finanziamento del terrorismo, e le informazioni "*di contrasto*", come i dati detenuti dalle autorità nazionali di prevenzione, indagine, accertamento e perseguimento dei reati. Rispetto a questi si definisce cosa si intende per "*reati gravi*", per riciclaggio, per "*reati presupposti associati*", tra cui è espressamente inclusa la criminalità informatica, nonché per finanziamento del terrorismo; di quest'ultimo viene, in particolare, data una definizione quale fornitura o raccolta fondi per la realizzazione di ben 21 categorie di reati espressamente contemplati.
Gli artt. da 3 a 9 individuano le Autorità nazionali competenti a richiedere le informazioni, nonché le procedure e tempistiche relative allo scambio d'informazioni con le autorità e le Unità d'intelligence finanziaria degli Stati Membri, nonché con Europol. Nello specifico, sono designate, tra le autorità nazionali competenti abilitate ad accedere al registro nazionale centralizzato dei conti bancari, l'Ufficio nazionale per il recupero dei beni istituito presso il Ministero dell'interno, il Capo della polizia - direttore generale della pubblica sicurezza, i questori, il direttore della Direzione investigativa antimafia, mentre il Nucleo speciale di polizia valutaria della Guardia di finanza e della Direzione investigativa antimafia sono individuati per la ricezione e richiesta delle informazioni finanziarie o analisi finanziarie detenute dall'UIF.
Gli artt. 10 e 11 fissano apposite disposizioni a garanzia del correttamente trattamento dei dati e del rispetto dei diritti degli interessati.

Schema decreto e relazione illustrativa

5. Schema del decreto legislativo di attuazione della direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale

Sulla scia dell'avvenuta comunicazione da parte della Commissione europea dell'avvio, nei confronti della Repubblica italiana, di una procedura di infrazione ex articolo 258 T.F.U.E. per mancato recepimento della direttiva in oggetto, nel Consiglio dei Ministri del 5 agosto 2021 è stato approvato e trasmesso alle Camere per i pareri del caso lo schema di decreto di attuazione.
Sulla base della relazione illustrativa, le modifiche normative portate dallo schema di decreto sarebbero meri interventi correttivi sostanzialmente conservativi della disciplina nazionale di contrasto al riciclaggio, in quanto si limiterebbero solo ad estendere il campo di applicazione delle norme nazionali dei delitti di riciclaggio, autoriciclaggio, impiego e ricettazione.
Relativamente a questi reati, lo schema del decreto prevede, infatti, solo l'estensione della cerchia dei reati presupposto, mediante inclusione, negli articoli da 648 a 648-*ter*.1 c.p., anche dei delitti colposi e delle contravvenzioni, con previsione per questi ultimi di una disciplina sanzionatoria apposita di minor rigore. Le ulteriori modifiche attengono, poi, all'allineamento sanzionatorio delle fattispecie emendate sul piano circostanziale; in proposito si segnala la riformulazione all'art. 648 c.p. della circostanza attenuante del fatto di particolare tenuità e l'introduzione dell'aggravante della commissione nell'esercizio di attività professionale. Rispetto a questa disposizione, sulla base della relazione risulta, inoltre, che il legislatore nazionale ha volutamente evitato d'intervenire sulla struttura del delitto di ricettazione, considerando, da un lato, la condotta sanzionata idonea a ricomprendere, anche, le condotte- oggetto degli obblighi d'incriminazione da attuare - di "detenzione e utilizzazione" nella consapevolezza della provenienza delittuosa; dall'altro, il fine di profitto non generativo di alcun effetto restrittivo che ne possa giustificare l'eliminazione.
Nulla è stato previsto in generale per la manifestazione informatica dei fatti di reato incriminati, nemmeno sul piano dell'oggetto materiale, nonostante la nozione ampia di "beni" portata dalla direttiva; anzi, sempre in

ordine al delitto di ricettazione, nella relazione il mantenimento del riferimento a "*cose provenienti da delitto*" è stato giustificato in considerazione dell'adozione da parte della recente giurisprudenza nazionale di una concezione di "*cosa*" dei delitti contro il patrimonio comprensiva dei dati informatici.
Anche relativamente alla sussistenza della giurisdizione italiana conformemente ai criteri fissati dalla direttiva, lo schema del decreto, a fronte di un giudizio di conformità delle disposizioni nazionali vigenti, prevede solo per i delitti di ricettazione e autoriciclaggio l'esclusione della condizione di procedibilità prevista dall'art. 9, comma 2, c.p., che in mancanza della modifica sarebbe applicabile sulla base dei limiti edittali previsti dagli articoli 648 e 648 e *ter* l c.p..

Schema del decreto e relazione illustrativa

6. Congiuntura e rischi del sistema finanziario italiano in una prospettiva comparata

Il Rapporto della Consob analizza la congiuntura e i rischi del sistema finanziario italiano nel confronto internazionale, tenendo anche in conto i processi innescati dalla crisi economica generata dalla pandemia di Covid-19 sui mercati azionari e obbligazionari e sul risparmio delle famiglie italiane.
Tra gli ambiti di analisi, un'autonoma considerazione è assegnata agli investimenti mediante cripto attività e, in generale, al ricorso agli strumenti di finanza decentralizzata, basata su infrastrutture che utilizzano la tecnologia *blockchain* e gli *smart contracts*.
Sulla base dei dati analizzati, risulta che nel 2021 si è registrato un significativo aumento soprattutto delle attività di *lending* ed un rilevante rialzo delle quotazioni di Bitcoin.
Oltra alla più marcata volatilità che connota queste forme d'investimento rispetto alle opzioni tradizionali, è messo in luce come questa crescita non sia, però, associata anche ad una conforme implementazione dei livelli di sicurezza informatica delle piattaforme di scambio e delle relative tecnologie sottostanti. Sulla base dei dati disponibili - relativi a 479 piattaforme digitali dedicate a cripto attività - emerge, infatti, come meno di 30 possono ritenersi molto affidabili per la qualità delle informazioni pubblicate e solo 7 ottengono una valutazione molto positiva in termini di sicurezza cibernetica. Ne deriva che rimane elevato il rischio di frodi e attacchi informatici, il quale sulla base di stime per il 2019 era già quantificato in 4,5 miliardi di dollari, in netta crescita rispetto al biennio precedente.

Rapporto Consob 2021

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Il reato di produzione di materiale pedopornografico prescinde dal consenso del minore raffigurato

Il reato di produzione di materiale pedopornografico di cui all'art. 600-*ter* co. 1 c.p. sussiste anche nell'ipotesi in cui la persona offesa minorenne ritratta nel video abbia prestato il suo consenso alla videoregistrazione dell'atto sessuale. Inoltre, la ripresa del compimento di atti sessuali espliciti è senz'altro ricompresa nel concetto di pedopornografia di cui all'art. 600-*ter* co. 7 c.p., in quanto costituisce materiale pedopornografico la rappresentazione, con qualsiasi mezzo atto alla conservazione, di atti sessuali espliciti coinvolgenti soggetti minori di età, oppure degli organi sessuali di minori con modalità tali da rendere manifesto il fine di causare concupiscenza od ogni altra pulsione di natura sessuale alla rappresentazione degli organi sessuali di un minore "per scopi sessuali". Peraltro, una videoripresa siffatta è certamente idonea a provocare nello spettatore il risveglio ovvero il rinnovo di istinti erotici, contestualmente al compiacimento legato alla visione del materiale così prodotto.

In senso conforme: 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, sentenza 4 agosto 2021, (ud. 16 giugno 2021), n. 30326/2021, Pres. Ramacci, Rel. Di Santi

2. Divulgare su *Whatsapp* i *selfie* di una minorenne nuda costituisce cessione di materiale pedopornografico

Integra il reato di cessione di materiale pedopornografico di cui all'art. 600-*ter* co. 4 c.p. la divulgazione tramite *Whatsapp* di *selfie* pedopornografici realizzati dallo stesso minore, in quanto, con riferimento a tale ipotesi delittuosa, non rileva la modalità della produzione del materiale pedopornografico, che ben può essere stato realizzato anche dallo stesso minore. Infatti, il principio di necessaria alterità tra l'agente autore del fatto ed il minore opera solo con riferimento alle condotte sanzionate dal co. 1 dell'art. 600-*ter* c.p., mentre negli altri casi il materiale pedopornografico può essere autoprodotto dal minore.

In senso conforme: Corte di Cassazione, sez. III penale, sentenza 12 febbraio 2020 (ud. 21 novembre 2019), n. 5522/2020 – Pres. Izzo, Rel. Macrì in *Newsletter febbraio2020,* con nota di 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.

Per approfondire: ROSANI D., «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.; 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.; SALVADORI I., *Sexting, minori e diritto penale*, in CADOPPI A., CANESTRARI S., MANNA A. e PAPA M.(a cura di), *Cybercrime*, Torino, 2019, p. 567 ss; ID., *I minori da vittime ad autori di reati di pedopornografia? Sui controversi profili penali del sexting*, in *Ind. pen.*, 2017, n. 3, 789 ss.; PICOTTI L., *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in BERTOLINO M., FORTI G. (a cura di), *Scritti per Federico Stella*, Napoli, 2007, vol. II, p. 1267 ss..

Corte di Cassazione, sez. III penale, sentenza 8 luglio 2021 (ud. 20 maggio 2021), n. 29579/2021, Pres. Ramacci – Est. Di Stati

3. L'ordinanza di rimessione alle Sezioni Unite in tema di produzione di materiale pedopornografico

La presente ordinanza di remissione alle Sezioni Unite della Corte di Cassazione trae origine dal ricorso dell'imputato, secondo cui la Corte territoriale avrebbe fornito un'erronea lettura della fattispecie di reato di pornografia minorile, contraria a quella stabilita dalla Sezione Unite nella sentenza n. 51815/2018. La Corte aveva infatti ritenuto che la minore, di anni quindici, fosse stata "utilizzata" dall'imputato per realizzare immagini pedopornografiche anche se questa aveva prestato il proprio consenso alla produzione del materiale. Secondo la difesa il consenso della minore deve considerarsi rilevante in quanto le Sezioni Unite hanno incentrato l'interpretazione della norma sul concetto di "utilizzazione". In effetti, con riguardo alle condotte rientranti nell'ambito dell'autonomia privata sessuale, le Sezioni Unite hanno concluso che è la condotta di utilizzazione del minore a circoscrivere l'area del penalmente rilevante, in quanto "presuppone la ricorrenza di un differenziale di potere tra soggetto che realizza le immagini e il minore rappresentato".
Tuttavia, la Corte nell'ordinanza di remissione rileva che, legittimando implicitamente il c.d. *sexting* primario, questo orientamento presenta il rischio di lasciare un vuoto di tutela coincidente con il *sexting* secondario, ossia con la successiva cessione o diffusione del materiale prodotto a soggetti estranei alla loro produzione, non ritenendosi sufficiente l'introduzione del reato di cui all'art. 612-*ter* c.p., che non si occupa esplicitamente della tutela dei minori.

La questione sollevata dalla terza Sezione riguarda quindi la produzione di materiale pornografico coinvolgente minori che hanno raggiunto l'età per esprimere il consenso sessuale, nelle diverse aree riguardanti la produzione del materiale e la successiva cessione e diffusione, in particolare quando i minori siano parte di una relazione interpersonale con un adulto, più difficilmente definibile quale paritaria.
Con questa ordinanza di remissione la Sezione III chiede quindi alle Sezioni Unite di approfondire le diverse aree del consenso del minore ultraquattordicenne, rivolgendo il seguente quesito: "se il reato di cui all'art. 600-*ter*, comma 1, n. 1, c. p. risulti escluso nell'ipotesi in cui il materiale pedo-pornografico sia prodotto, ad esclusivo uso privato delle persone coinvolte, con il consenso di persona minore, che abbia compiuto gli anni quattordici, in relazione ad atti sessuali compiuti nel contesto di una relazione affettiva con persona minorenne che abbia la capacità di prestare un valido consenso agli atti sessuali, ovvero con persona maggiorenne".

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; 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.; SALVADORI I., *Sexting, minori e diritto penale*, in CADOPPI A., CANESTRARI S., MANNA A. e PAPA M. (a cura di), *Cybercrime*, Torino, 2019, p. 567 ss.; ROSANI D., «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, ordinanza 1° luglio 2021 (ud. 22 aprile 2021), n. 25334 - Pres. Marini, Rel. Rosi.

4. La pubblicazione *online* di una sentenza accompagnata da commenti offensivi costituisce diffamazione

Commette il reato di diffamazione colui che pubblica su un sito *Internet* da lui gestito una sentenza penale evidenziando i punti riferiti alla vita affettiva dell'imputata e aggiungendo chiose e commenti deplorevoli e volgari relativi a quest'ultima. Il carattere diffamatorio della pubblicazione si desume dal richiamo in termini umilianti e dileggianti della relazione intrattenuta dalla donna con il dirigente dell'ufficio, strumentalizzata al fine di denigrare e offendere l'onore di quest'ultima. L'uso di espressioni volgari e offensive esclude la continenza delle forme usate e, dunque, la sussistenza della scriminante del diritto di critica.

Per approfondire: PICOTTI L., *Profili penali delle comunicazioni illecite via Internet*, in *Dir. inf. inf.*, 1999, n. 2, p. 283 ss.; CORRIAS LUCENTE G., *Il diritto penale dei mezzi di comunicazione di massa*, Padova, 2000; CASSANO G., SGROI M., *La diffamazione civile e penale*, Milano, 2011.

Corte di Cassazione, sez. V penale, sentenza 22 luglio 2021 (ud. 1 giugno 2021), n. 28634/2021, Pres. De Gregorio – Rel. Caputo

5. Riferibilità del profilo Facebook in caso di reato di diffamazione online

In relazione ad un reato di diffamazione realizzato sul social network Facebook veniva contestava la riferibilità della condotta all'imputata essendo stata omessa ogni indagine sui file di log, indirizzo IP e dati informatici, a prescindere dal nickname utilizzato, risultando quindi basata su prove non certe. La motivazione fonderebbe sulla mera riferibilità del profilo all'imputata, sulla circostanza logica del contenuto dei post che riportavano fatti della vita privata della parte lesa. A sostegno di tale posizione parte ricorrente richiama un precedente della Corte di legittimità secondo cui era stato ritenuto necessario l'accertamento dell'IP per la certa riferibilità del post.
La Corte di legittimità, evidenziando come il precedente richiamato si rifacesse ad un caso diverso, in cui era controversa l'intestazione dell'IP riferibile al profilo Facebook registrato a nome di persona diversa, evidenzia come la costante giurisprudenza della Corte di legittimità si attesta sulla riferibilità della diffamazione anche su base indiziaria, a fronte della convergenza, pluralità e precisione di dati quali il movente, l'argomento del forum su cui avviene la pubblicazione, il rapporto tra le parti, la provenienza del post dalla bacheca virtuale

dell'imputato, con utilizzo del suo nickname, anche in mancanza di accertamenti circa la provenienza del post di contenuto diffamatorio dall'indirizzo IP dell'utenza telefonica intestata all'imputato medesimo. Si è, inoltre, attribuito rilievo, assieme agli elementi indiziari sopra sottolineati, anche all'assenza di denuncia di cd. furto di identità da parte dell'intestatario della bacheca sulla quale vi è stata la pubblicazione dei post incriminati.

In senso conforme: Corte di Cassazione, sez. V penale, sentenza 9 ottobre 2018 (ud. 13 luglio 2018), n. 45339/2018 - Pres. Pezzullo, Rel. Settembre; Corte di Cassazione, sez. V, sentenza 1° marzo 2016 (ud. 13 luglio 2015) n. 8328/2016 - Pres. Bruno, Rel. Pezzullo.

Corte di Cassazione, sez. V penale, sentenza 21 giugno 2021 (ud. 21 gennaio 2021), n. 24212 - Pres. Vessichelli, Rel. Calaselice

6. L'accesso abusivo al sistema informatico da parte del dipendente in possesso delle credenziali

Ai fini della configurabilità del reato di accesso abusivo ad un sistema informatico, qualora il soggetto agente sia dotato delle credenziali per accedere ad una banca dati riservata è necessario accertare se la condotta addebitata all'imputato esuli o meno dalle competenze dell'operatore, ponendosi in contrasto con le prescrizioni relative all'accesso e al trattenimento nel sistema informatico, contenute in disposizioni organizzative impartite dal titolare dello stesso, indipendentemente dalle finalità soggettivamente perseguite. In particolare, qualora l'accesso non sia finalizzato ad acquisire conoscenza di atti di altro ufficio o di informazioni riservate perché avente oggetto un atto proprio del dipendente, la giurisprudenza di merito deve chiarire perché si tratterebbe di un accesso ontologicamente inibito, nel senso di attività svolta per finalità estranee alle ragioni di istituto e agli scopi sottostanti alla protezione dell'archivio informatico, illustrando in che modo vi sarebbe stato sviamento di potere, individuando la norma organizzativa asseritamente violata e spiegando perché l'accesso sarebbe ontologicamente inibito, in quanto incompatibile con le mansioni del dipendente.

In senso conforme: Corte di Cassazione, sez. unite penali, sentenza 8 settembre 2017 (ud. 18 maggio 2017), n. 41210/2017, Pres. Canzio - Rel. Savani; Corte di Cassazione, sez. unite penali, sentenza 7 febbraio 2012 (ud. 27 ottobre 2011), n. 4694/2012, Pres. Lupo - Rel. Fiale.

Per approfondire: SALVADORI I., *I reati contro la riservatezza informatica*, in CADOPPI A., CANESTRARI S., MANNA A. e 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 *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, p. 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 PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 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, p. 21 ss..

Corte di Cassazione, sez. V penale, sentenza (ud. 17 maggio 2021), n. 26530/2021, Pres. Sabeone – Rel. Belmonte

7. Non sussiste *overruling* giurisprudenziale *in malam partem* in materia di accesso abusivo a sistema informatico

Commette il reato di accesso abusivo a sistema informatico aggravato ex art. 615-*ter* co. 2 n. 1 e 3 c.p. la condotta del militare della Guardia di Finanza che, abusando della *password* e della matricola meccanografica a lui assegnate, accede alle banche dati della Guardia di Finanza senza alcuna autorizzazione e senza che ricorresse alcuna ragione di servizio, in quanto, non essendo egli assegnato a funzioni operative, non era legittimato ad accedere ad alcuna banca dati. Tale condotta, per le sue connotazioni abusive, sarebbe stata penalmente rilevante anche alla stregua dell'orientamento giurisprudenziale precedente alla sentenza 'Savarese' delle Sezioni Unite. Invero, le Sezioni Unite 'Casani' avevano già affermato il principio secondo

cui commette il delitto previsto dall'art. 615-*ter* c.p., colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema. Pertanto, si deve escludere la sussistenza di un *overruling in malam partem*.

In senso conforme: Corte di Cassazione, sez. unite penali, sentenza 8 settembre 2017 (ud. 18 maggio 2017), n. 41210/2017, Pres. Canzio - Rel. Savani; Corte di Cassazione, sez. unite penali, sentenza 7 febbraio 2012 (ud. 27 ottobre 2011), n. 4694/2012, Pres. Lupo - Rel. Fiale.

Per approfondire: SALVADORI I., *I reati contro la riservatezza informatica*, in CADOPPI A., CANESTRARI S., MANNA A. e 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 *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, p. 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 PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 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, p. 21 ss..

Corte di Cassazione, sez. V penale, sentenza 6 luglio 2021 (ud. 30 aprile 2021), n. 19186/2021, Pres. Pezzullo – Rel. Riccardi

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

Nagni E., *Artificial intelligence, l'innovativo rapporto di (in)compatibilità fra machina sapiens e processo penale*

Altre riviste

Delvecchio F., *L'informazione della giustizia penale*, in *Riv. Trim. Dir. Pen. Cont.*, 2021, n. 2, p. 60 ss.

Kostoris R.E., *Predizione decisoria, diversion processuale e archiviazione*, in *Riv. Trim. Dir. Pen. Cont.*, 2021, n. 2, p. 42 ss.

Lavorgna A. e Suffia G., *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, in *Riv. Trim. Dir. Pen. Cont.*, 2021, n. 2, p. 88 ss.

Salvadori I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista italiana di diritto e procedura penale*, 2021, n. 1, p. 83 ss.

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