NEWS ON CYBERCRIME

News luglio – dicembre 2022

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

NOVITÀ SOVRANAZIONALI

1. Regolamento sui servizi digitali

È stato pubblicato il regolamento europeo sui servizi digitali (UE) 2022/2065 del 19 ottobre 2022 (c.d. *Digital Service Act*), che dovrà applicarsi dal 14 febbraio 2024. Il regolamento, finalizzato a contribuire al corretto funzionamento del mercato interno dei servizi digitali, stabilisce norme armonizzate per un ambiente online sicuro, prevedibile, affidabile, volto a facilitare l'innovazione. Esso si applica ai servizi intermediari offerti a destinatari stabiliti nell'Unione o che sono ubicati nell'Unione, indipendentemente dal luogo di stabilimento dei prestatori di tali servizi.
L'impostazione del regolamento segue quella della direttiva 2000/31/CE, che viene fatta salva. Rimane quindi la modulazione della responsabilità e degli obblighi degli intermediari in base al servizio offerto, a seconda che sia di mero trasporto o di memorizzazione di informazioni.
Per tutelare e garantire che l'ambiente online sia trasparente e sicuro, vengono previsti obblighi diversificati per gli intermediari. Mentre tutti i soggetti devono prevedere dei punti di contatto per le autorità competenti nonché per i destinatari dei propri servizi, obblighi più precisi vengono previsti a carico dei prestatori di servizi di memorizzazione di informazioni, comprese le piattaforme online (prestatori che memorizzano e diffondono informazioni al pubblico). Tra questi, i più rilevanti consistono nell'obbligo di predisporre un meccanismo di segnalazione e azione in relazione a contenuti illegali, l'obbligo di notifica di sospetti di reati alle autorità giudiziarie competenti, nonché le misure contro gli abusi dei propri servizi da parte di quegli utenti che con frequenza forniscono contenuti manifestamente illegali.
Vi è infine una sezione dedicata agli obblighi specifici previsti a carico dei fornitori di piattaforme online e di motori di ricerca online di dimensioni molto grandi per la gestione dei rischi sistemici. *(B.P.)*

Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)

2. Regolamento sui mercati digitali (Digital Market Act)

È stato pubblicato il 14 settembre 2022 il nuovo regolamento europeo sui mercati digitali (c.d. *Digital Market Act*), che dovrà applicarsi dal 2 maggio 2023. Il regolamento prevede nuovi obblighi a carico dei *gatekeepers*, piattaforme digitali che forniscono servizi di piattaforma di base (servizi di intermediazione online; motori di ricerca; servizi di *social network*; servizi per la condivisione di video; servizi di comunicazione interpersonale indipendenti dal numero; sistemi operativi; *browserweb*; assistenti virtuali; servizi di *cloud computing*; servizi pubblicitari online), che abbiano un impatto significativo sul mercato interno; oppure che forniscano un servizio che costituisce un punto di accesso (*gateway*) importante affinché gli utenti commerciali raggiungano gli utenti finali; oppure che detengano una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisiscano siffatta posizione nel prossimo futuro. Il regolamento disciplina una serie di obblighi in capo a tali soggetti, affinché venga garantita una concorrenza leale sulle proprie piattaforme.
Il regolamento europeo mira quindi a creare un contesto più equo per gli utenti commerciali che dipendono dai *gatekeepers* per offrire i loro servizi nel mercato unico digitale. In tal modo, i consumatori disporranno di servizi più numerosi, della possibilità di cambiare più facilmente fornitore se lo desiderano, nonché di un accesso diretto ai servizi e a prezzi più equi.
Il regolamento si applica ai servizi di piattaforma di base forniti o offerti dai *gatekeeper* a utenti commerciali stabiliti nell'Unione o a utenti finali stabiliti o situati nell'Unione, a prescindere dal luogo di stabilimento o di residenza dei *gatekeeper*. *(B.P.)*

Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali)

3. Direttiva NIS II

Sta per concludersi l'iter legislativo europeo di approvazione e pubblicazione della proposta di direttiva relativa a misure dirette a garantire un livello comune elevato di *cyber*-sicurezza nell'Unione (c.d. direttiva NIS 2), che sostituisce e abroga la direttiva (UE) 2016/1148 (c.d. direttiva NIS).
La Direttiva NIS 2 introduce nuove regole finalizzate a promuovere un elevato livello di sicurezza informatica comune nell'UE, sia per le aziende che per gli Stati membri. La necessità di aggiornare il quadro legislativo fermo al 2016 è da ricondursi al ruolo sempre più significativo che ricopre la *cyber*-sicurezza nella società contemporanea, fattore abilitante fondamentale per molti settori critici, portatore dei vantaggi economici, sociali e sostenibili della digitalizzazione.
La normativa fissa obblighi di sicurezza informatica più severi per i paesi dell'UE. Tale misura punta altresì a migliorare la cooperazione tra gli stessi, anche in caso di incidenti su larga scala, sotto l'egida dell'Agenzia dell'UE per la sicurezza informatica (ENISA). Si amplia inoltre il ventaglio di soggetti interessati dagli obblighi della direttiva. Vengono incluse società, tra le altre, che offrono servizi sanitari (come società farmaceutiche e produttori di dispositivi medici) e servizi di produzione, trasformazione e distribuzione di cibo. Mentre la Direttiva NIS lasciava alla discrezionalità degli Stati l'individuazione dei soggetti su cui ricadevano gli obblighi in materia di *cyber*-sicurezza, la NIS 2 definisce in modo più dettagliato la categoria dei soggetti cui si rivolge, definiti "soggetti essenziali e importanti", seguendo un criterio uniforme per la loro identificazione, dato dall'applicazione di una soglia di medie o grandi dimensioni (salvo per determinate piccole imprese e microimprese che soddisfano criteri specifici e che ricoprono un ruolo chiave per la società, l'economia o per particolari settori o tipi di servizi). Tutti tali soggetti devono adottare misure tecniche**,** operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che essi utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. A loro carico vengono previsti anche obblighi di segnalazione all'autorità competente nonché al proprio CSIRT (*Computer Security Incident Response Team*), di cui vengono inoltre definiti in modo più preciso i requisiti**,** le capacità tecniche e i compiti. *(B.P.)*

Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)

4. Proposta del *Cyber Resilience Act*

La proposta della Commissione del c.d. *Cyber Resilience Act* si origina dalla mancanza di una regolamentazione nell'attuale quadro giuridico dell'UE della *cyber*-sicurezza del *software* non incorporato. Gli attacchi alla *cyber*-sicurezza prendono infatti sempre più di mira le vulnerabilità di tali prodotti, causando costi sociali ed economici significativi. Esistono numerosi esempi di attacchi informatici di grande portata dovuti a una sicurezza non ottimale dei prodotti, come il *worm ransomware* WannaCry, che ha sfruttato una vulnerabilità di Windows.
Il regolamento proposto stabilirebbe: norme per l'immissione sul mercato di prodotti con elementi digitali per garantirne la *cyber*-sicurezza; requisiti essenziali per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali; obblighi in materia di *cyber*-sicurezza per gli operatori economici in relazione a tali prodotti; requisiti essenziali per i processi di gestione delle vulnerabilità messi in atto dai fabbricanti; obblighi per gli operatori economici in relazione a tali processi; nonché norme sulla vigilanza del mercato e sull'applicazione delle norme e dei requisiti previsti.
I destinatari di tale proposta di regolamento comprendono gli operatori dell'intero ciclo di vita di tali prodotti: dal fabbricante, all'importatore, al distributore. I fabbricanti in particolare dovrebbero effettuare una valutazione della conformità del prodotto con elementi digitali e dei processi messi in atto per determinare se siano soddisfatti i requisiti essenziali, elencati nell'allegato I della proposta di regolamento. *(B.P.)*

Proposta di regolamento europeo relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, COM(2022) 454 final

5. Rapporto dell'Ufficio dell'Alto Commissario delle Nazioni Unite per i diritti umani, "Il diritto alla privacy nell'era digitale"

Il rapporto esamina le recenti tendenze e sfide riguardanti il diritto alla *privacy*. Il rapporto si concentra, in particolare, su: (a) l'abuso di strumenti di *hacking* invasivi; (b) il ruolo chiave della crittografia nel garantire la tutela del diritto alla *privacy* e di altri diritti; (c) il monitoraggio diffuso degli spazi pubblici. Il documento evidenzia il rischio di creare sistemi di sorveglianza e controllo pervasivi che possono violare diversi beni giuridici tutelati dagli ordinamenti nazionali e internazionali.
Il report si concentra in particolare sullo *spyware* Pegasus, uno degli esempi che rende maggiormente evidente la crescita di un panorama di *spyware* commercializzati dalle aziende ai governi di tutto il mondo. Secondo alcuni studi di settore, almeno 65 governi hanno acquistato strumenti di sorveglianza *spyware* commerciali. L'azienda produttrice ha dichiarato di annoverare tra i propri clienti 60 agenzie governative in 45 Paesi. Pochi giorni prima delle rivelazioni di Pegasus, Citizen Lab e Microsoft hanno pubblicato un rapporto che descriveva dettagliatamente come un altro *software*, Candiru, fosse stato utilizzato dai governi per colpire difensori dei diritti umani, dissidenti, giornalisti, attivisti e politici.
Anche se si perseguono obiettivi legittimi, come la sicurezza nazionale o la protezione dei diritti altrui, la valutazione della necessità e della proporzionalità dell'uso dei *software* spia limita fortemente gli scenari in cui questi sarebbero ammissibili. Vi sono forti argomentazioni sul fatto che strumenti come Pegasus, che consentono intrusioni senza limiti nella vita delle persone, potrebbero intaccare l'essenza del diritto alla *privacy* e interferire con i diritti alla libertà di pensiero e di opinione. Considerati gli impatti negativi sostanziali dell'uso dei *software* spia, nonchè la loro portata, il report afferma che il loro uso dovrebbe essere limitato ai casi in cui servirebbero a prevenire o indagare su un reato grave specifico o su un atto che rappresenta una grave minaccia per la sicurezza nazionale. Il loro utilizzo dovrebbe essere strettamente mirato a un'indagine sulla persona o sulle persone sospettate di commettere o aver commesso tali atti. Dovrebbero quindi costituire l'ultima risorsa. Le misure adottate dovrebbero anche essere soggette a una rigorosa supervisione indipendente; è essenziale l'approvazione preventiva da parte di un organo giudiziario. L'Alto commissariato delle Nazioni Unite per i diritti umani ribadisce un suo recente appello, così come quello di esperti e gruppi per i diritti umani, volto ad incentivare una moratoria sulla vendita, il trasferimento e l'uso di strumenti di *hacking* fino a quando non sarà in vigore un regime di salvaguardie basato sui diritti umani. *(B.P.)*

Annual report of the United Nations, High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, "The right to privacy in the digital age", 4 August 2022

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Proposta di riconoscere rango costituzionale al diritto di accesso ad Internet

Il 13 ottobre 2022 è stata presentata alla Camera dei Deputati una proposta di legge costituzionale (iniziativa on. Madia) che intende modificare l'art. 21 della Costituzione per riconoscere il diritto di accesso alla rete Internet. La proposta è dettata dalla consapevolezza, resa ancora più evidente negli anni di pandemia, che "l'accesso alla rete internet rappresenta, oggi, uno degli spartiacque tra inclusione ed esclusione sociale", costituendo una componente essenziale della cittadinanza. Le tre finalità della proposta, si legge nella relazione, sono: garantire l'accesso ai servizi digitali; favorire la possibilità di formazione dei singoli e delle formazioni sociali; promuovere lo sviluppo dell'economia digitale e la nascita di nuove professionalità e opportunità di lavoro. Si propone quindi di aggiungere alla fine dell'art. 21 Cost. il seguente comma: "Tutti hanno eguale diritto di accedere alla rete internet, in condizioni di parità, con modalità tecnologicamente adeguate tali da favorire la rimozione di ogni ostacolo di ordine economico e sociale. La legge stabilisce provvedimenti adeguati a prevenire le violazioni del diritto di cui al presente comma". *(B.P.)*

Per approfondire: RODOTÀ S., *Una Costituzione per Internet*?, in *Politica del diritto*, 2010, n. 3, p. 337 ss.

Proposta di legge costituzionale. Atto Camera n. 327

2. La riforma Cartabia e la tutela del diritto all'oblio

Con l'entrata in vigore della riforma del processo penale di cui alla legge 27 settembre 2021, n. 134 nonché del d.lgs. 10 ottobre 2022, n. 150 di attuazione delle deleghe in essa contenute, è stata ulteriormente rafforzata la tutela del diritto all'oblio di coloro che sono stati assolti nel processo penale. Il nuovo art. 64-*ter* delle disposizioni attuative del codice di procedura penale, infatti, prevede che il decreto di archiviazione e la sentenza di non luogo a procedere o di assoluzione costituiscano titolo per l'emissione di un provvedimento di deindicizzazione che, nel rispetto della normativa dell'Unione europea in materia di dati personali, garantisca in modo effettivo il diritto all'oblio degli indagati o imputati. Il provvedimento di deindicizzazione può essere chiesto ed ottenuto dalla cancelleria del giudice che ha emesso la sentenza di assoluzione o il decreto di archiviazione. Inoltre, è possibile chiedere anche una deindicizzazione preventiva, ossia l'obbligo di rendere non indicizzabili dai motori di ricerca tutti gli articoli che siano scritti da quel momento in poi. *(C.C.)*

Art. 41 decreto legislativo 10 ottobre 2022, n. 150 di attuazione della legge 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Autoriciclaggio tramite l'acquisto di criptovalute

Rientra nella nozione di "attività speculativa" penalmente rilevante ai fini della commissione del reato di autoriciclaggio di cui all'art. 648 *ter*.1 c.p. anche l'acquisto di criptovalute con denaro proveniente da un reato, dato che nella nozione di "attività speculativa" possono rientrare tutte quelle attività in cui il soggetto ricerca il raggiungimento di un utile, anche assumendosi il rischio di considerevoli perdite. Inoltre, le valute virtuali possono essere utilizzate per scopi diversi dal pagamento e comprendere prodotti di riserva di valore a fini di risparmio ed investimento. *(C.C.)*

Corte di cassazione, sez. II penale, sentenza 13 luglio 2022, (ud. 7 luglio 2022), n. 27023

2. I rapporti tra i reati in materia di pornografia minorile

Secondo la giurisprudenza richiamata dalla Corte nella pronuncia sotto indicata, il reato di detenzione di materiale pornografico di cui all'articolo 600 *quater* c.p. e quello di pornografia minorile *ex* articolo 600 *ter* c.p., che ne incrimina la produzione e la diffusione, non integrano due distinti illeciti, ma due diverse modalità di realizzazione del medesimo reato, con la conseguenza che non possono concorrere tra loro se riguardano il medesimo materiale, mentre può sussistere il concorso se il materiale oggetto della produzione e quello oggetto della detenzione siano diversi.
Nel caso di specie i giudici di merito hanno escluso che il delitto di detenzione di materiale pedopornografico potesse essere ritenuto assorbito in quello di diffusione di cui all'articolo 600 *ter* comma 3 c.p., in considerazione dell'ingente quantitativo di materiale detenuto dal ricorrente, presente in cartelle deputate all'archiviazione, ulteriori e diverse da quelle deputate alla condivisione via Internet.
La Corte di legittimità ha ritenuto che sia stato correttamente configurato il concorso tra i reati contestati di detenzione e diffusione del materiale, posto che l'assai ingente quantitativo di immagini pedopornografiche detenute dall'imputato, diverse e ulteriori rispetto a quelle diffuse, costituisce condotta distinta, dotata di una sua propria carica di offensività, cosicché è stata affermata la configurabilità di entrambe le fattispecie di reato, in considerazione della autonomia delle condotte e della loro indipendente idoneità a compromettere, in modo diverso, il bene protetto.
Nella pronuncia si ribadisce inoltre la linea di discrimine tra le due fattispecie di diffusione e cessione di materiale pedopornografico: si avrà infatti il delitto di cui all'articolo 600 *ter* comma 3 c.p., nel caso in cui il soggetto inserisca foto pornografiche raffiguranti minori in un sito liberamente accessibile ovvero quando le

propaghi per mezzo della rete Internet, inviandole ad un gruppo o ad una lista di discussione da cui chiunque le possa scaricare, mentre è configurabile l'ipotesi più lieve di cui all'articolo 600 *ter* comma 4 c.p., quando l'agente invia le foto a una persona determinata, allegandole ad un messaggio di posta elettronica oppure tramite il profilo Facebook del destinatario, in modo tale che solo quest'ultimo abbia la possibilità di prelevarle. *(B.P.)*

In senso conforme: Corte di Cassazione, sez. III penale, 22 ottobre 2020 (ud. 6 novembre 2019), n. 2252; Corte di Cassazione, sez. III penale, 15 gennaio 2019 (ud. 27 settembre 2018), n. 1647.

Corte di Cassazione, sez. III penale, 11 ottobre 2022 (ud. 20 settembre 2022), n. 38178

3. La definizione di "materiale pedopornografico"

La Corte richiama la definizione di pornografia minorile di cui all'articolo 600 *ter* u.c. c.p. ("ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attivita' sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali"), affermando che la norma contiene due ipotesi distinte tra loro: nella prima rientra qualsiasi rappresentazione del minore di anni diciotto che sia coinvolto in attività sessuali esplicite, reali o simulate, realizzate da qualunque soggetto, a prescindere dall'età; nella seconda, più specifica e limitata, rientra qualunque, cioè ogni forma di rappresentazione degli organi sessuali di un minore di anni diciotto che sia finalizzata a scopi sessuali.
Nella prima ipotesi della norma rientrano quelle rappresentazioni in cui il minore non sia solo l'autore delle attività sessuali, che devono essere esplicite, cioè emergere chiaramente dalle rappresentazioni, ma anche quelle in cui sia trascinato, associato, interessato, reso partecipe in essa quando queste siano attuate da soggetti terzi, minorenni o maggiorenni. La Corte evidenzia che il concetto di attività sessuali è più ampio di quello di atto sessuale rilevante *ex* articolo 609 *bis* c.p., perché concerne qualunque esplicazione, qualunque condotta concernente la sfera sessuale da parte di un singolo o di più soggetti.
Nel caso di specie, la rappresentazione dell'esibizione degli organi genitali da parte di un adulto, che si alza allo scopo il vestito per mostrarsi nuda all'obiettivo, realizzata rendendo ad essa partecipe il minore, associato nell'immagine, concretizza il compimento di attività sessuali esplicite con il minore, rilevante *ex* articolo 600 *ter* c.p..
Per quanto riguarda la seconda ipotesi prevista dalla norma, ad essa sono state ricondotte foto in cui la vittima è ritratta da sola, mentre mostra il pube, anche se coperto, ritenendo non necessaria la nudità quale presupposto per l'applicazione dell'articolo 600 *ter* u.c. c.p.. Si è dato rilievo, in particolare, all'oggetto della rappresentazione, il pube, ed alla posa fatta assumere alla minore - che aveva le gambe allargate - sicché si è ritenuto che le foto siano state scattate esclusivamente per una finalità sessuale. Pertanto, la presenza delle "mutandine" non è stata ritenuta di per sé rilevante, dal momento che l'oggetto della rappresentazione é l'organo sessuale della minore, oltre a doversi rilevare che tali capi di abbigliamento non sono necessariamente coprenti o comunque possono consentire ugualmente la visione, totale o parziale, degli organi sessuali.
A supporto della tesi esposta viene richiamata dalla Corte la tutela ulteriore accordata dalla legge ai minori anche dall'articolo 600 *quater*.1 c.p.. Tale norma punisce infatti le condotte di produzione di materiale pedopornografico e la detenzione dello stesso, quando il materiale "rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse", specificando che "per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali". *(B.P.)*

Corte di Cassazione, sez. III penale, 27 ottobre 2022 (ud. 6 luglio 2022), n. 40609

4. La nozione di identità digitale rilevante ai sensi dell'art. 640-*ter* co. 3 c.p.

In tema di frode informatica, la nozione di "identità digitale" di cui all'art. 640-*ter* co. 3 c.p. nonostante l'assenza di una definizione legislativa non presuppone una procedura di validazione adottata dalla pubblica amministrazione. Tale interpretazione, infatti, è destituita di giuridico fondamento in quanto contrasta sia con la constatazione empirica circa l'esistenza di diverse tipologie di identità digitale, caratterizzate da soglie differenziate di sicurezza in relazione alla natura delle attività da compiere nello spazio virtuale, sia, soprattutto, con la ratio della disposizione in questione, volta a rafforzare la fiducia dei cittadini

nell'utilizzazione dei servizi *online* e a porre un argine al fenomeno delle frodi realizzate soprattutto nel settore del credito al consumo mediante il furto di identità. Pertanto, la circostanza aggravante trova applicazione anche nel caso di utilizzo di credenziali di accesso a sistemi informatici a gestione privatistica quale i servizi di *home banking* o le piattaforme di vendita *online*. *(C.C.)*

In senso conforme: Corte di Cassazione, sez. II penale, sentenza 11 agosto 2020 (ud. 2 luglio 2020), n. 23760

Per approfondire: CRESCIOLI C., *La tutela penale dell'identità digitale*, in *Dir. Pen. Cont*., 2018, n. 5, p. 265 ss.; MALGIERI G., *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo,* in *Dir. pen. cont.- Riv. trim.,* n. 2, 2015, p. 143 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**.**

Corte di Cassazione, sez. II penale, sentenza 27 ottobre 2022 (ud. 20 settembre 2022), n. 40862

5. Accesso abusivo a un sistema informatico da parte di un pubblico ufficiale

Nella pronuncia sotto indicata la Corte richiama la giurisprudenza delle Sezioni Unite in materia di accesso abusivo ad un sistema informatico. Il caso di specie può essere infatti interpretato secondo i principi formulati nella sentenza delle Sezioni Unite Savarese (Sez. U, n. 41210 del 18/05/2017), che ha precisato la direzione esegetica espressa dalle Sezioni Unite Casani (Sez. U, n. 4694 del 27/10/2011, dep. 2012). Secondo la pronuncia del 2017, integra il delitto previsto dall'articolo 615 *ter* comma 2, n. 1 c.p., la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso gli è attribuita.
Nella recente pronuncia si è quindi approfondito e specificato il concetto di "operazioni ontologicamente estranee" a quelle consentite, qualora la condotta criminosa sia posta in essere da un pubblico ufficiale o da un incaricato di pubblico servizio. Nel caso di specie la Corte, richiamando la precedente giurisprudenza, evidenzia che, anche laddove manchino regole specifiche disciplinanti il funzionamento e l'utilizzo della banca dati pubblica che viene in considerazione, il requisito della violazione di legge sussiste non solo quando la condotta del pubblico ufficiale sia svolta in contrasto con le norme che regolano l'esercizio del potere, ma anche quando la stessa risulti orientata - sviando dal potere conferito - alla sola realizzazione di un interesse collidente con quello per il quale il potere è attribuito. *(B.P.)*

In senso conforme: Corte di Cassazione, sez. Unite penali, 7 febbraio 2012 (ud. 27 ottobre 2011), n. 4694; Corte di. Cassazione, sez. Unite penali, 8 settembre 2017 (ud. 18 maggio 2017), n. 41210.

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.; 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, 28 ottobre 2022 (ud. 27 settembre 2022), n. 40882

6. Jihad elettronica e partecipazione nel reato di organizzazione terroristica

Dal momento che la disposizione incriminatrice di cui all'art. 270 *bis* c.p. non precisa gli indici di riconoscibilità dell'attività di "partecipazione" a una associazione "con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico", e non esiste una nozione astratta di "partecipazione", valida per ogni tipo di reato associativo, la modalità della "partecipazione" medesima è correlata alle caratteristiche proprie dell'entità cui si "partecipa". Ciò vale soprattutto per l'organizzazione denominata Stato Islamico. L'organizzazione terroristica transnazionale assume infatti le connotazioni, più che di una struttura statica, di una "rete" in grado di mettere in relazione soggetti assimilati da un comune progetto politico-militare, che funge da catalizzatore dell'"affectio societatis" e costituisce lo scopo sociale del sodalizio. In altri termini, adotta un modello "polverizzato" di articolazione.

Nel caso di specie la partecipazione all'Isis è stata desunta, tra gli altri: dalla detenzione su supporti informatici di materiale jihadista; dal sistematico e costante uso del *web* e dei *social media* per condividere e diffondere messaggi di propaganda e di indottrinamento, nonché video relativi a gravi episodi di violenza, reperiti nel cd. *deep web*, attraverso canali accessibili solo mediante specifiche chiavi informatiche; dall'aver fornito assistenza ad un associato, ospitato per lungo tempo presso un centro culturale presieduto dall'imputato.
Da tali elementi si è ritenuto l'imputato responsabile del delitto di partecipazione ad associazione con finalità di terrorismo internazionale *ex* art. 270 *bis* c.p., e non del delitto di istigazione a delinquere *ex* art. 414 c.p., trattandosi di condotte di un soggetto che può qualificarsi quale aperto sostenitore del c.d. Stato islamico e rispondenti alla chiamata al *jihad*, strumentali al consolidamento ed al rafforzamento dell'organizzazione
A detta della Corte, non si tratta di plurime forme di manifestazione di un pensiero politico-religioso, sia pure estremo, oggetto di possibile tutela ai sensi della previsione dell'art. 21 Cost., ma di un concreto e variegato atteggiarsi nel mondo esterno della (interiore) condivisione ideologica delle finalità dell'associazione, in relazione alla quale assumono valore centrale i principi dell'integralismo religioso musulmano di matrice sunnita e di ispirazione salafita, la cui applicazione si traduce in un'inevitabile e, nella prospettiva dell'Isis, necessaria lesione del bene giuridico protetto dall'articolo 270 *bis* c.p.. *(B.P.)*

In senso conforme: Corte di Cassazione, sez. V penale, 2 maggio 2022 (ud. 18 genino 2022), n. 17079; Corte di Cassazione, sez. V penale, 5 marzo 2020 (ud. 18 dicembre 2020), n. 8891; Corte di Cassazione, sez. II penale, 21 maggio 2019 (ud. 21 febbraio 2019), n. n. 22163.

Per approfondire: GOVERNA J., *Jihad elettronica e partecipazione nel reato di organizzazione terroristica ex art. 270-bis c.p.*, in *Diritto di Internet*, 2021, n. 3, p. 523 ss.

Corte di Cassazione, sez. II penale, 18 novembre 2022 (ud. 11 ottobre 2022), n. 43917

7. Abusivismo finanziario e *bitcoin*

Con riguardo all'uso della moneta virtuale come mezzo di scambio o strumento finanziario, ove la vendita di *bitcoin* venga reclamizzata come una vera e propria proposta di investimento, si ha un'attività soggetta agli adempimenti di cui agli artt. 91 ss. TUF, la cui omissione integra il reato di cui all'art. 166 comma 1 lett. c) TUF, che punisce chiunque, senza esservi abilitato ai sensi del decreto "offre fuori sede, ovvero promuove o colloca mediante tecniche di comunicazione a distanza, prodotti finanziari o strumenti finanziari o servizi o attività di investimento".
Nel caso di specie la raccolta di fondi aveva avuto come scopo la creazione di una piattaforma decentralizzata di servizi logistici, e da chi aveva contribuito era stata corrisposta in cambio moneta virtuale, che costituiva titolo per l'utilizzo dei servizi della piattaforma.
La Corte ritiene sussistenti i caratteri distintivi dell'investimento di tipo finanziario, dati dalle circostanze per cui gli agenti: a) avevano erogato capitali (sotto la forma di *bitcoin*); b) con l'aspettativa di ottenere un rendimento, costituito dalla corresponsione di altre monete virtuali che avrebbero permesso la partecipazione alla piattaforma, dal valore variabile a seconda del momento dell'acquisto e che avrebbe acquistato maggior valore se il progetto relativo alla piattaforma avesse avuto successo; c) avevano assunto su di sé un rischio connesso al capitale investito. La valuta virtuale deve quindi essere considerata nel caso di specie quale strumento di investimento in quanto consiste in un prodotto finanziario. *(B.P.)*

In senso conforme: Corte di Cassazione, sez. II penale, sentenza 25 settembre 2020 (ud. 17 settembre 2020), n. 26807.

Per approfondire: VADALÀ R. M., *La disciplina penale degli usi ed abusi delle valute virtuali*, in *Diritto di Internet*, 2020, n. 3, p. 397 ss.; ID., *La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale*, in *Giurisprudenza italiana*, 2021, n. 10, p. 2225 ss.; ID., *La funzione d'investimento e le valute virtuali: scenari di repressione penale*, in *Diritto di internet*, 1/2022, p. 119 ss..

Corte di Cassazione, sez. II penale, sentenza 22 novembre 2022 (ud. 26 ottobre 2022), n. 44378

8. La responsabilità penale del blogger per la mancata rimozione dei commenti offensivi

L'amministratore di un sito Internet, in particolare di un *blog*, non può essere ritenuto responsabile per la diffamazione ai sensi dell'art. 57 c.p., dato che tale norma è applicabile alle sole testate giornalistiche telematiche e non anche ai diversi mezzi informatici di manifestazione del pensiero (*forum*, *blog*, *newsletter*, *newsgroup*, *mailing list*, *facebook*, ecc.). Tuttavia, è responsabile a titolo di concorso nella diffamazione aggravata dal mezzo della pubblicità per gli scritti di carattere denigratorio pubblicati sul proprio sito da terzi quando, venutone a conoscenza, non provveda tempestivamente alla loro rimozione, atteso che tale condotta equivale alla consapevole condivisione del contenuto lesivo dell'altrui reputazione e consente l'ulteriore diffusione dei commenti diffamatori. *(C.C.)*

In senso conforme: Corte di Cassazione, sez. V penale, sentenza 20 marzo 2019 (ud. 8 novembre 2018), n. 12546

Per approfondire: PANATTONI B., *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel cyberspace*, in *Sist. Pen*., 22 maggio 2020; PAGELLA C., *La Cassazione sulla responsabilità del blogger per contenuti diffamatori (commenti) pubblicati da terzi*, in *Dir. Pen. Cont*., 17 maggio 2019

Corte di Cassazione, sez. V penale, sentenza 1° dicembre 2022, (ud. 21 settembre 2022), n. 45680

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, 12 settembre 2022

SALVI G., *Attuazione della giurisdizione penale nello spazio virtuale e sicurezza nazionale*, 15 novembre 2022

Diritto di Internet

BARRESI O., *La nuova rilevanza penale del trattamento illecito dei dati personali: il ripristino del principio di extrema ratio tra il detto e non detto della suprema corte*, 2022, n. 4, p. 767 ss.

CHIARAVIGLIO P., L*a circolazione di idee discriminatorie ed i social network, tra apprezzamento, condivisione e comunità criminali virtuali*, 2022, n. 4, p. 759 ss.

SOANA G., *Criptoriciclaggio: un orientamento che si consolida*, 2022, n. 4, p. 749 ss.

Altre riviste e contributi

GIANNINI A., *Intelligenza artificiale, human oversight e responsabilità penale: prove d'impatto a livello europeo*, in *Discrimen*, 21 novembre 2022

PANATTONI B., *Violazioni "incorporee" della sfera sessuale. Possibili evoluzioni ed insidie nell'ambito dei reati sessualmente connotati*, in *Archivio Penale*, 2 dicembre 2022

PICOTTI L., *Cybercrimes and criminal relevance of artificial intelligence*, in *La transformación algorítmica del sistema de justicia penal*, 2022, n. 7, p. 67 ss.