

NEWS ON

News marzo – giugno 2022

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

NOVITÀ SOVRANAZIONALI

1. IOSCO e rischi del mercato finanziario on line retail

La *International Organization of Securities Commissions* (IOSCO) ha aperto a marzo 2022 una consultazione per l'elaborazione di soluzioni regolamentari al passo con l'evoluzione tecnologica del mercato finanziario retail, che sappiano fronteggiare le minacce connesse, quali la presenza di **numerosi operatori abusivi, non soggetti alla giurisdizione di origine dell'investitore**.

Viene, altresì, messo in luce come i **social network** siano sempre più spesso utilizzati per reperire informazioni finanziarie o per perpetrare vere e proprie condotte illecite, come **manipolazioni o truffe**, nel caso di diffusione loro tramite di informazioni false o ingannevoli su prodotti e investimenti finanziari o di realizzazione di veri e propri **schemi ponzi o c.d. international romance scams**, in cui il legame amoroso o di amicizia viene utilizzato come esca per consigliare finte attività di trading. Tra le altre innovative tecniche fraudolente riguardanti gli investimenti on line vengono indicate, anche, **truffe di criptovalute, c.d. bolier room scam (c.d. truffe in locale caldaia)**, che si hanno quando società di investimento impiegano società separate, collocate in altra giurisdizione, che attraverso call center, chat online, e-mail o social media, offrono azioni o obbligazioni senza valore o addirittura inesistenti. Nel caso invece di una **clone investment firms**, società sprovviste delle necessarie autorizzazioni usano il nome o altri dati di una nota società autorizzata o addirittura ne clonano il sito web, inserendo il collegamento a piattaforme di trading false. Un'altra forma di frode diffusa è quella denominata **pump and dump**, in cui promotori cercano prima di aumentare il prezzo di un'azione con dichiarazioni false o fuorvianti ed una volta che il prezzo è salito, per trarre profitto la rivendono. Altri tipi di frode e truffa osservati in quest'ambito riguardano la **sottrazione da parte di piattaforme di trading dei fondi loro affidati o la realizzazione non autorizzata e altamente speculativa di attività di gestione del portafoglio online**. Rispetto a fenomeni criminali di questo tipo, il report indica come possibile strumento da utilizzare per identificarli e reprimerli efficacemente il ricorso a **tecniche di monitoraggio dei social media mediante tecnologia AI/ML (Artificial Intelligence/Machine Learning) o webscraping** (tecnica informatica di estrazione dati da un sito web per mezzo di programmi software che simulano la navigazione umana). (R.M.V.)

[Retail Market Conduct Task Force Consultation Report IOSCO](#)

2. Le autorità di regolamentazione del settore finanziario dell'UE mettono in guardia i consumatori sui rischi delle crypto-attività

Con un avvertimento congiunto in data 17 marzo 2022 le Autorità europee di vigilanza (ABE, ESMA e EIOPA – le AEV) hanno messo in guardia i consumatori sull'acquisto di crypto attività, rappresentando come non si tratta solo del rischio di **perdere tutto il capitale investito** a causa della complessità o dei movimenti estremi dei prezzi di questi prodotti e servizi o di casi di **manipolazione di mercato e pubblicità ingannevole**, ma di cadere altresì vittima di **frodi**, ovvero del **furto o smarrimento delle chiavi private** che forniscono l'accesso alle relative attività, od ancora di subire disservizi o errori operativi o finanche di veri e propri **attacchi informatici**, senza poter beneficiare della protezione esistente ai sensi delle attuali norme UE sui servizi finanziari. (R.M.V.)

[EU financial regulators warn consumers on the risks of crypto-assets](#)

3. La Corte di Giustizia UE si esprime in materia di data retention

Sulla base dell'art. 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al **trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche**, come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letto alla luce degli **articoli 7, 8 e 11 e dell'articolo 52**, paragrafo 1, della **Carta dei diritti fondamentali dell'Unione europea**, sono legittime le misure legislative nazionali che prevedano, per **finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica**, sia la **conservazione temporalmente limitata allo stretto necessario, ma rinnovabile, e mirata**, sulla base di elementi oggettivi e non discriminatori, dei dati relativi al traffico e all'ubicazione di mezzi di comunicazioni elettronica, sia la **conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione e dell'identità civile degli utenti di questi mezzi di comunicazione elettronica, per un periodo temporalmente limitato allo stretto necessario**. In questa ottica di bilanciamento proporzionato, per le medesime finalità e purché in presenza di norme chiare e precise sulle condizioni sostanziali e procedurali e delle garanzie effettive a favore delle persone interessate contro il rischio di abusi, la Corte reputa, altresì, **legittimo il ricorso a un'ingiunzione** - emessa da autorità competente, anche fin dal primo atto d'indagine, e soggetta a un controllo giurisdizionale effettivo - **rivolta ai fornitori di servizi di comunicazione elettronica, di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui essi dispongono**, anche se riguardanti persone diverse da quelle sospettate, ma che anteriormente al verificarsi di una minaccia grave per la sicurezza pubblica o alla commissione di un atto di criminalità grave, abbiano avuto contatti con la vittima attraverso mezzi di comunicazione elettronica. Per la Corte **non è conforme** al quadro delineato la **normativa irlandese che rimette**, peraltro, **il trattamento centralizzato delle domande, provenienti dalla polizia nell'ambito della ricerca e del perseguimento di reati gravi, di accesso a dati conservati dai fornitori di servizi di comunicazione elettronica, ad un funzionario di polizia**, ancorché assistito da un'unità istituita all'interno della polizia che gode di una certa autonomia e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale. Questo soggetto non rivestendo la qualità di terzo rispetto a tali domande, **non soddisfa i requisiti di indipendenza e di imparzialità che sono stati individuati proprio con riferimento all'ambito penale**. In presenza di una normativa di questo tipo il giudice nazionale deve procedere ad una declaratoria d'invalidità totale, e l'eventuale ammissibilità degli elementi di prova ottenuti in forza della disciplina dichiarata invalida, va determinata, conformemente al principio di autonomia procedurale degli Stati membri, sulla base del diritto nazionale, sempreché nel rispetto dei principi di equivalenza e di effettività. (R.M.V.)

[Corte di Giustizia dell'Unione Europea, sez. grande, 5 aprile 2022, C-140/20](#)

4. Direttiva copyright e tutela della libertà d'espressione

La Corte di Lussemburgo si è occupata nella pronuncia in commento della legittimità dell'**art. 17 della direttiva 2019/790** sul diritto d'autore e sui diritti connessi nel mercato unico digitale, il quale prevede che i **fornitori di servizi di condivisione di contenuti online** siano direttamente responsabili nel caso in cui materiali protetti dal **diritto d'autore** siano caricati illegalmente dai propri utenti. Con ricorso presentato alla Corte, la Polonia ha infatti chiesto l'annullamento (parziale, o, in subordine, totale) del suddetto articolo in quanto sarebbe stato contrastante con la tutela del diritto alla libera manifestazione del pensiero (art. 11 Carta di Nizza). In particolare, è stato contestato che il regime previsto dal **paragrafo 4 dell'art. 17**, secondo cui i fornitori di servizi, per andare esenti da responsabilità, hanno l'obbligo di compiere i massimi sforzi, da un lato, per assicurare che non siano disponibili contenuti protetti specifici per i quali i titolari di diritti abbiano fornito le informazioni pertinenti e necessarie e, dall'altro, per impedire che i contenuti protetti oggetto di una segnalazione sufficientemente motivata da parte di tali titolari **siano caricati in futuro**, costringa gli stessi fornitori di servizi ad operare una **sorveglianza preventiva tramite filtraggi automatici dei contenuti**, con **grave pregiudizio delle libertà d'espressione e d'informazione**.

Pur riconoscendo che il regime previsto dalla norma europea comporta effettivamente una limitazione dell'esercizio del diritto alla libertà di espressione e d'informazione degli utenti di tali servizi di condivisione, la Corte afferma che tale **limitazione deve ritenersi legittima e giustificata**, secondo i criteri previsti dall'**art. 52 della Carta di Nizza**, in virtù del complesso-regime previsto dall'art. 17, comprensivo di paragrafi

successivi (da 7 a 10), contenenti correttivi che mirano a garantire che la limitazione della libertà d'espressione sia espressamente prevista dalla legge nei suoi contenuti e nelle sue modalità, nonché debba essere necessaria e proporzionata al contro-interesse che si intende tutelare: in questo caso, la proprietà intellettuale. (B.P.)

[Corte di Giustizia dell'Unione Europea, sez. grande, 26 aprile 2022, C-401/19](#)

5. Amazon e la tutela del marchio nelle conclusioni dell'Avvocato generale MACIEJ SZPUNAR

Le questioni al vaglio della Corte di Giustizia, poste dal *Tribunal d'arrondissement de Luxembourg* nella causa C-148/21 e dal *Tribunal de l'entreprise francophone de Bruxelles* nella causa C-184/21, riguardano ancora una volta la **responsabilità degli intermediari che gestiscono piattaforme di vendita online per violazioni dei diritti di proprietà intellettuale** e specificamente di quelli discendenti da marchio registrato. Si tratta in particolare di verificare la **responsabilità diretta** di un gestore di una piattaforma di vendite online, come Amazon, **per offerte di prodotti contraffatti**, stabilendo se sia direttamente riferibile al predetto gestore l'uso da parte sua, **ai sensi dell'articolo 9 del regolamento 2017/1001**, di un segno identico a un marchio registrato. L'Avvocato generale propone alla Corte di interpretare la predetta norma in modo che **non si possa ritenere che il gestore di una piattaforma di vendite online usi un marchio nel contesto di un'offerta di vendita pubblicata da un terzo** su detta piattaforma, in ragione del fatto che, da una parte, pubblica in maniera uniforme sia le proprie offerte sia offerte di terzi senza distinguerle nella loro visualizzazione in base alla rispettiva origine, facendo comparire il proprio logo di noto distributore su detti annunci sia sul proprio sito sia nelle sezioni pubblicitarie di siti Internet di terzi; e, dall'altra, offre ai venditori terzi servizi complementari di assistenza, di stoccaggio e di spedizione dei prodotti pubblicati sulla sua piattaforma, informando i potenziali acquirenti che si farà carico della fornitura di tali servizi, a condizione che tali elementi non inducano un utente di Internet normalmente informato e ragionevolmente attento a percepire il marchio di cui trattasi come parte integrante della comunicazione commerciale del gestore. Alla base delle conclusioni proposte dall'Avvocato generale vi è il riconoscimento della riferibilità ad Amazon delle statuizioni adottate in precedenza dalla Corte di Giustizia con riguardo ad operatori come eBay e quindi l'esclusione di uso vietato del segno registrato nel quadro della propria comunicazione commerciale in considerazione del fatto che, pur operando Amazon sia come distributore di grande notorietà, sia come mercato online, **all'interno degli annunci è sempre specificato se i prodotti sono venduti da venditori terzi o direttamente da Amazon** e per gli utenti della piattaforma è nota la presenza di entrambe le tipologie di offerte. Con riguardo poi ai servizi aggiuntivi sulle vendite di terzi offerti da Amazon, si ritiene che non possano determinare una sua responsabilità diretta per violazione delle prerogative riguardanti il marchio perché se è vero che **il maggior controllo esercitato in questo modo dall'impresa rileva dal punto di vista delle norme di diritto dell'Unione in materia di commercio elettronico, non vale, però, automaticamente anche per l'interpretazione della nozione di «uso»** controversa nel caso di specie. Per l'Avvocato generale **una questione è qualificare il servizio fornito dal gestore di una piattaforma di vendite online** ai fini del riconoscimento di un suo ruolo attivo, di conoscenza e controllo della legittimità dei contenuti delle offerte e quindi eventualmente di una sua **responsabilità secondaria o indiretta**, **altra è stabilire se la sua attività sia anche idonea a determinare un «uso» vietato di un segno registrato** all'interno della propria comunicazione commerciale e quindi **una responsabilità diretta**. Questa differenziazione è, in particolare, collegata alla **diversità degli interessi in gioco**, i quali attengono nel caso controverso esclusivamente alla **protezione dei diritti del titolare del marchio** di cui trattasi. (R.M.V.)

[Conclusioni dell'Avvocato generale del 2 giugno 2022 nelle cause riunite C-148/21 e C-184/21](#)

6. Regolamento relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito

Con il regolamento 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 è stata approvata la proposta di regolamento su un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito (COM(2020) 594 final). Alla luce dei considerando 2, 4 e 5 questo regolamento è stato emanato, in particolare, nella duplice consapevolezza che *“la maggior parte delle cripto-attività non rientra nell'ambito di applicazione della legislazione dell'Unione in materia di servizi finanziari”*, e che *“la legislazione dell'Unione in materia di servizi finanziari non è stata concepita tenendo conto della tecnologia a registro distribuito e delle cripto-attività, e contiene disposizioni che potenzialmente precludono o limitano l'uso della*

*tecnologia a registro distribuito nell'emissione, nella negoziazione e nel regolamento delle cripto-attività che rientrano nella definizione di strumenti finanziari (...). Allo stesso tempo, esistono lacune normative dovute a specificità giuridiche, tecnologiche e operative connesse all'uso della tecnologia a registro distribuito e alle cripto-attività che rientrano nella definizione di strumenti finanziari. Per esempio, non sono stati imposti requisiti di trasparenza, affidabilità o sicurezza ai protocolli e agli «smart contract», che sono alla base delle cripto-attività che rientrano nella definizione di strumenti finanziari. **La tecnologia sottostante potrebbe anche comportare nuove forme di rischi che non sono adeguatamente affrontati dalle norme vigenti**”.*

Alla luce di quanto sopra viene definito come **strumento finanziario DLT** (Distributed ledger technology, in italiano, tecnologia a registro distribuito) quello strumento che è tale ai sensi dell'articolo 4, paragrafo 1, punto 15, della direttiva 2014/65/UE ed è “emesso, registrato, trasferito e stoccato mediante la tecnologia a registro distribuito”. Si definisce per tale “una tecnologia che consente il funzionamento e l'uso dei registri distribuiti” e per **infrastruttura di mercato DLT** un “sistema multilaterale di negoziazione DLT, sistema di regolamento DLT o sistema di negoziazione e regolamento DLT”. Il regolamento fissa, inoltre, i requisiti per: a) la concessione e la revoca di autorizzazioni specifiche a operare le infrastrutture di mercato DLT in conformità del presente regolamento; b) la concessione, la modifica e la revoca delle esenzioni alle autorizzazioni specifiche; c) l'imposizione, la modifica e la revoca delle condizioni legate a esenzioni; d) la gestione delle infrastrutture di mercato DLT; e) la vigilanza delle infrastrutture di mercato DLT; e f) la collaborazione tra i gestori delle infrastrutture di mercato DLT, le autorità competenti e l'Autorità europea degli strumenti finanziari e dei mercati. Relativamente a questa collaborazione è prescritto che i **gestori delle infrastrutture di mercato DLT devono notificare senza indugio alle loro autorità competenti, anche, “qualsiasi prova di accesso non autorizzato, malfunzionamento rilevante, perdita, attacchi informatici o altre minacce cibernetiche, frode, furto o altri gravi abusi subiti”**. In generale, il regolamento prescrive in funzione di prevenzione di queste minacce un regime di **affidabilità cibernetica** degli operatori che si avvalgono di infrastrutture di mercato DLT, il cui rispetto può essere soggetto alla verifica dell'autorità competente, mediante la nomina di un revisore indipendente incaricato a tal fine. E' prescritto, in particolare, che questi operatori garantiscano che **tutti i dispositivi informatici e cibernetici** relativi all'uso della loro tecnologia a registro distribuito siano **proporzionati alla natura, alla portata e alla complessità delle loro attività**, nonché **assicurino la continuità e la costante trasparenza, disponibilità, affidabilità e sicurezza dei loro servizi** e delle loro attività, compresa l'**affidabilità degli smart contract** utilizzati nell'infrastruttura di mercato DLT. Ulteriore garanzia deve essere prestata anche in ordine all'**integrità, alla sicurezza e alla riservatezza di tutti i dati memorizzati dai gestori in questione**. E', inoltre, imposto che **tutti i dispositivi informatici e cibernetici in uso garantiscano che i fondi, le garanzie reali e gli strumenti finanziari DLT** detenuti da una infrastruttura di mercato DLT, nonché i relativi mezzi di accesso, siano **protetti dai rischi di accesso non autorizzato, pirateria informatica, degrado, perdita, attacco informatico, furto, frode, negligenza e altri gravi malfunzionamenti operativi**. (R.M.V.)

[Regolamento \(UE\) 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 che modifica i regolamenti \(UE\) 600/2014 e \(UE\) 909/2014 e la direttiva 2014/65/UE](#)

7. Modificato il c.d. Regolamento Europol

Considerata la rapida evoluzione che ha segnato il panorama della sicurezza in Europa, sempre più gravemente minacciata da forme di **criminalità grave, organizzata e transnazionale**, che si servono in sempre più larga misura dei progressi delle **tecnologie digitali**, le istituzioni europee hanno **esteso i compiti di Europol** con il regolamento 2022/991 dell'8 giugno 2022, riconoscendo il ruolo sempre più essenziale che l'agenzia europea svolge anche quale nesso di collegamento e cooperazione tra le diverse autorità nazionali. Infatti, si legge tra i considerando che hanno condotto all'approvazione del regolamento in esame, che “i criminali hanno dimostrato di sapere adattare le loro modalità operative e sviluppare nuove attività criminali in tempi di crisi, anche facendo ricorso a strumenti che si servono della tecnologia per moltiplicare ed espandere la gamma e la portata delle loro attività criminali”. Le modifiche apportate al **regolamento 2016/794** attribuiscono dunque a Europol compiti aggiuntivi così da consentirle di sostenere meglio le autorità competenti nazionali degli Stati membri, preservando appieno le competenze degli Stati membri nel settore della sicurezza nazionale. Oltre alla cooperazione tra Europol e le autorità nazionali, emerge anche l'esigenza di sviluppare modelli di coordinamento tra le **diverse agenzie europee**. In particolare, nelle azioni volte alla prevenzione e al contrasto del crimine informatico, specialmente quello che si sostanzia in **attacchi informatici su larga scala** che

prendono di mira soggetti sia pubblici che privati, colpendo vari settori, fra cui i trasporti, la sanità e i servizi finanziari, Europol dovrebbe cooperare con l'ENISA (**l'Agenzia dell'Unione europea per la cibersicurezza**), in specie attraverso scambi di informazioni e fornendo supporto analitico nei settori che rientrano nelle rispettive competenze.

Diverse disposizioni sono dedicate a stabilire regole in relazione ai processi di trattamento dati svolti da Europol. Tra queste, particolarmente rilevante risulta l'introduzione degli **articoli 18 bis, 26 bis e 26 ter**. Rispettivamente, il primo si occupa di regolare i processi di trattamento dei dati personali svolti da Europol a sostegno delle indagini penali. L'art. 26 bis è dedicato invece alla facoltà data ad Europol di ricevere e trattare dati personali direttamente da parti private in "**situazioni di crisi online**", ossia (secondo la definizione data dall'**art. 2 lett. t**) nel caso di diffusione di contenuti online relativi a un fatto in corso o recente del mondo reale che ritraggono un danno alla vita o all'integrità fisica o che richiama un danno imminente alla vita o all'integrità fisica e che hanno l'obiettivo o l'effetto di intimidire gravemente la popolazione, a condizione che vi sia un legame o un ragionevole sospetto di legame con il terrorismo o l'estremismo violento e che si preveda la moltiplicazione esponenziale e la viralità di tale contenuto tra vari servizi online. Infine, l'art. 26 ter disciplina la facoltà di Europol di ricevere e trattare dati personali direttamente da parti private nell'ambito di attività volte a affrontare la diffusione online di materiale pedopornografico. (B.P.)

[Regolamento \(UE\) 2022/991 dell'8 giugno 2022 che modifica il regolamento \(UE\) 2016/794 per quanto riguarda la cooperazione di Europol con le parti private, il trattamento dei dati personali da parte di Europol a sostegno di indagini penali, e il ruolo di](#)

8. Proposta di nuovo regolamento europeo in materia di cybersecurity

La Commissione europea ha proposto il **22 marzo 2022** un nuovo regolamento (che si allineerebbe alla legislazione esistente, che ricomprende, in particolare, la direttiva (UE) 2016/1148, c.d. direttiva NIS) per istituire un quadro che garantisca norme e **misure comuni in materia di cibersicurezza** nelle istituzioni, negli organi e nelle agenzie dell'Unione, con lo scopo di migliorare le capacità di resilienza e di risposta agli incidenti di tutti i soggetti in questione. Tra le principali novità si segnala il **rafforzamento del mandato del gruppo per la preconfigurazione di una squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'UE (c.d. CERT-UE)**, che dovrebbe essere rinominato in **centro per la cibersicurezza**. Inoltre con la proposta di regolamento in esame si intende richiedere alle istituzioni, organi, uffici e agenzie dell'UE di: disporre di un quadro di riferimento per la governance, la gestione del rischio e il controllo nel settore della sicurezza informatica; implementare una base di misure di cybersecurity che affrontino i rischi identificati; condurre valutazioni periodiche della maturità delle misure; mettere in atto un piano per migliorare la propria cybersecurity; condividere le informazioni relative agli incidenti con il CERT-EU senza ritardi ingiustificati.

Infine, si istituirebbe un comitato interistituzionale per la cibersicurezza (*Interinstitutional Cybersecurity Board, IICB*). (B.P.)

[Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione, 23 marzo 2022, COM\(2022\) 122 final](#)

9. Intellectual Property Crime Threat Assessment 2022

Il rapporto realizzato congiuntamente da **Europol** ed Euipo, l'**Ufficio dell'Unione europea per la proprietà intellettuale**, mette in luce come i **crimini contro la proprietà intellettuale**, oltre a costituire una **minaccia per la salute e la sicurezza dei consumatori**, rappresentano un **business del crimine organizzato** in costante e rapida crescita a partire dalla pandemia, nel corso della quale la **distribuzione online e offline di merci contraffatte** è stata una delle principali attività criminali. Si è registrato, in particolare, un aumento della **vendita di prodotti contraffatti legati alla prevenzione o cura dell'infezione da Covid-19**, come prodotti sanitari e farmaceutici, compresi falsi vaccini, tramite varie **piattaforme online e social media**, con espansione dell'e-commerce business-to-consumer. Queste vendite sono state realizzate non solo nel **dark web**, in cui la loro commercializzazione è stata spesso associata all'impiego di criptovalute, ma anche nel **surface web**: anzi è risultato ed è proprio quest'ultimo ad ospitare le principali piattaforme di distribuzione di

merci contraffatte di ogni tipo. Altro settore che il report indica come particolarmente interessato da questo tipo di reati è quello alimentare, della c.d.. “**agromafia**”.

A prescindere dal tipo di prodotto contraffatto, in generale, le organizzazioni dedite a queste attività criminali sono estremamente ramificate, soprattutto quelle cinesi, aventi legami con le principali organizzazioni europee. Esse, inoltre, si affidano ad una **varietà di esperti tra cui operatori IT, grafici, chimici, medici, farmacisti, tecnici e consulenti finanziari**. A quest’ultimi sono affidati gli ingenti proventi da riciclare mediante operazioni sempre più sofisticate, che coinvolgono **criptovalute, investimenti off shore, finanziamento di attività ad alta intensità di denaro o acquisto di beni di lusso**.

Oltre al **riciclaggio**, questi fenomeni criminali si associano a **furti d’identità**, in quanto la commercializzazione on line di questi prodotti avviene anche mediante siti che si spacciano o usano abusivamente il marchio di aziende note nel settore di afferenza. (R.M.V.)

[Europol-Euipo IP crime marzo 2022](#)

10. Rafforzato il codice di condotta sulla disinformazione

Il 16 giugno 2022 è stata adottata la versione rafforzata del **codice di buone pratiche** per le piattaforme online, le associazioni di categoria e i principali operatori del settore pubblicitario per **contrastare la disinformazione e migliorare le loro politiche online**, adottato per la prima volta nel 2018.

Mentre il codice del **2018**, con **16 firmatari**, prevedeva impegni basati sull’**auto-regolamentazione**, inerenti il vaglio degli inserzioni pubblicitarie, l’integrità dei propri servizi, la responsabilizzazione dei consumatori, nonché dei verificatori di fatti e dei ricercatori, la versione rafforzata, con **34 firmatari, 44 impegni e 127 misure specifiche**, si richiama alle forme di **co-regolamentazione** cui sono soggette le piattaforme online di dimensioni molto grandi nel quadro della normativa sui servizi digitali (**Digital Service Act**). Il codice rafforzato si prefigge inoltre di aumentare l’incisività delle misure e della trasparenza della pubblicità politica e tematica, nonché di garantire una sorveglianza completa dei comportamenti manipolativi attuali ed emergenti.

Tra gli impegni maggiormente rilevanti, si prevede di ampliare e rafforzare gli strumenti che consentono agli utenti di individuare e segnalare contenuti falsi o fuorvianti, istituire un solido quadro di monitoraggio e comunicazione, istituire un centro per la trasparenza e creare una task force permanente per l’evoluzione e l’adeguamento del codice. (B.P.)

[The Strengthened Code of Practice on Disinformation 2022](#)

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. La creazione del gruppo di lavoro per la riforma del processo penale telematico e dell’ufficio per il processo penale

Il 14 aprile 2022, con decreto del Ministro della Giustizia, è stato costituito **il gruppo di lavoro per l’elaborazione degli schemi di decreto legislativo in materia di processo penale telematico e di ufficio per il processo penale**, in attuazione della legge delega n. 134/2021 di riforma del processo penale. Tale gruppo di lavoro si affianca ai cinque gruppi di lavoro costituiti con decreto del 28 ottobre 2021 e di esso fanno parte studiosi ed esperti con differenti professionalità ed esperienze: docenti universitari di procedura penale, di informatica e di informatica giuridica, avvocati, magistrati, personale della Direzione generale per i Sistemi informativi automatizzati – D.G.S.I.A del ministero della Giustizia e personale amministrativo delle cancellerie e delle segreterie degli uffici giudiziari.

[Decreto 14 aprile 2022 - Costituzione del Gruppo di lavoro per l’attuazione della legge delega in materia di processo penale telematico e di ufficio per il processo penale](#)

1. Adescamento di minore online da parte dell'insegnante non diretto

La Cassazione, dopo aver confermato che la fattispecie di adescamento di minori di cui all'art. 609-undecies c.p. non pone problemi di legittimità costituzionale, in quanto **reato di pericolo concreto**, volto a neutralizzare il rischio di commissione dei più gravi reati a sfondo sessuale lesivi del corretto sviluppo psicofisico del minore e della sua autodeterminazione, ancorato a parametri oggettivi da cui possa dedursi il movente sessuale della condotta, conferma la condanna dell'imputato per avere adescato un **minore di anni 16, alunno nell'istituto scolastico nel quale egli era insegnante e vicario del preside, mediante l'utilizzo della chat di un social, con espressioni lusinghiere volte a capirne la fiducia**, domande volte a comprenderne l'orientamento sessuale, terminologie e frasi a riferimento sessuale. Trattandosi di un minore di età compresa tra i 14 e i 16 anni, l'elemento soggettivo in relazione al reato-scopo di atti sessuali con minorenni deve abbracciare anche il **rapporto di affidamento richiesto dall'art. 609-quater c. 1 n. 2 c.p.** La Cassazione precisa dunque che la condizione di affidamento per ragioni di istruzione, di vigilanza o di custodia prevista per il reato di atti sessuali con minorenni può avere carattere temporaneo o occasionale, potendo configurarsi **anche quando il soggetto attivo non sia l'insegnante diretto del minore, ma appartenga comunque alla stessa struttura scolastica**, all'interno della quale venga a diretto contatto con la vittima in ragione dell'incarico di svolgere lezioni o sostituzioni nelle varie classi. Inoltre, il rapporto di affidamento esistente tra insegnante ed alunno non può essere ritenuto escluso per il fatto che gli atti illeciti oggetto dell'imputazione si svolgano fuori dall'ambiente e dall'orario scolastico, perché ciò che conta è la relazione che sussiste fra i due soggetti, evidentemente non circoscrivibile al solo contesto in cui nasce e si manifesta principalmente. E ciò vale anche nel caso in cui il reato di atti sessuali con minorenni rilevi come reato-scopo ai fini della configurabilità di quello di adescamento.

In senso conforme: Corte di Cassazione, sez. III penale, sentenza 23 aprile 2019, (ud. 31 gennaio 2019), n. 17373/2019, Pres. Rosi - Rel. Gentili; Corte di Cassazione, sez. III penale, sentenza 13 luglio 2018, (ud. 15 marzo 2018), n. 32170/2018, Pres. Di Nicola - Rel. Andronio. (B.P.)

Corte di Cassazione, sez. III penale, sentenza 22 marzo 2022 (ud. 27 ottobre 2021), n. 9735/2022, Pres. Lapalorcia – Rel. Andronio

2. Atti persecutori e reiterata pubblicazione di fotografie su Facebook

Integra il reato di **atti persecutori ex art. 612-bis c.p., la pubblicazione ripetuta su Facebook della fotografia dell'ex compagna**, valutata unitamente alle condotte persecutorie commesse negli anni precedenti, tra cui i contatti ripetuti via *mail* e su *Facebook* anche con falsi profili, poiché **presenta un'evidente natura molesta**, dato che tale pubblicazione, anche in ragione della sua notevole capacità diffusiva, **contribuisce a creare un clima idoneo a compromettere la serenità e la libertà psichica della persona offesa**. Infatti, rientra nella **nozione di molestia**, quale elemento costitutivo del reato, qualsiasi condotta che concretizzi una indebita ingerenza o interferenza, immediata o mediata, nella vita privata e di relazione della vittima, attraverso la creazione di un clima intimidatorio ed ostile idoneo a comprometterne la serenità e la libertà psichica, anche attraverso il reiterato inserimento di *post sui social networks*.

In senso conforme: Corte di Cassazione, sez. V penale, sentenza 17 gennaio 2022 (ud. 16 settembre 2021), n. 1753/2022, Pres. Settembre – Rel. Guardiano; Corte di Cassazione, sez. V penale, sentenza 17 gennaio 2022 (ud. 17 novembre 2021), n. 1813/2022, Pres. Palla – Rel. Riccardi.

Corte di Cassazione, sez. V penale, sentenza 24 marzo 2022 (ud. 23 novembre 2021), n. 10680/2022, Pres. De Gregorio – Rel. Guardiano

3. Adescamento di minori e intervento del genitore

Integra il reato di **adescamento di minori** la condotta di colui che intrattiene con una minore di anni dieci **conversazioni a sfondo sessuale nella chat di un sito di giochi online**, chiedendole di scaricare un'applicazione per l'invio di fotografie, in modo da poter ricevere foto della minore a sfondo pornografico.

Infatti, nel caso in cui vi sia l'intervento di un genitore che scopra la *chat* e denunci immediatamente il fatto, **si consuma proprio ed esclusivamente il reato di adescamento di minori**, dato che non sono configurabili i reati sessuali più gravi indicati come reati scopo nell'art. 609-undecies c.p.

Per approfondire: BOGGIANI M., *L'adescamento di minorenni*, in CADOPPI A., CANESTRARI S., MANNA A. e PAPA M. (a cura di), *Cybercrime*, Torino, 2019, p. 599 ss.; SALVADORI I., *L'adescamento di minori. Il contrasto al child-grooming tra incriminazione di atti preparatori ed esigenze di garanzia*, Torino, 2018.

Corte di Cassazione, sez. III penale, sentenza 29 marzo 2022 (ud. 9 febbraio 2022), n. 11305/2022, Pres. Lapalorcia – Rel. Macrì

4. La disciplina transitoria per l'accesso ai dati del traffico telefonico è compatibile con la normativa europea

La **disciplina transitoria in materia di tabulati telefonici**, dettata dalla L. 23 novembre 2021, n. 178, che **consente l'utilizzabilità**, a carico dell'imputato, dei dati relativi al traffico telefonico, telematico e alle chiamate senza risposta, acquisiti nei procedimenti penali in data precedente alla data di entrata in vigore della nuova disciplina legislativa, **non è in contrasto col diritto dell'Unione Europea, a condizione che questi siano valutati unitamente ad altri elementi di prova ed esclusivamente per l'accertamento dei reati ivi indicati**. Infatti, **la stessa Corte di Giustizia** ha evidenziato che l'obiettivo di evitare che informazioni ed elementi di prova ottenuti in modo illegittimo arrechino indebitamente pregiudizio a una persona sospettata di avere commesso dei reati **può essere raggiunto non solo mediante un divieto di utilizzare informazioni ed elementi di prova siffatti**, ma anche mediante norme e prassi nazionali che disciplinino la valutazione e la ponderazione delle informazioni e degli elementi di prova, o addirittura tenendo conto del loro carattere illegittimo in sede di determinazione della pena. Pertanto, poiché la disciplina transitoria, quale "compensazione" rispetto alla mancanza di un provvedimento di acquisizione, consente l'utilizzabilità di tali dati solo in presenza di altri elementi di prova, è pienamente legittima.

Corte di Cassazione, sez. III penale, sentenza 1° aprile 2022 (ud. 31 gennaio 2022), n. 11991/2022, Pres. Marini – Rel. Andreazza

5. Posta elettronica ordinaria e diffamazione

La suprema Corte, quale giudice di legittimità che può però procedere in caso di diffamazione a considerare la sussistenza o meno della materialità della condotta contestata, ribadisce come **l'utilizzo della posta elettronica non esclude la sussistenza del requisito della "comunicazione con più persone"** anche nella ipotesi di diretta ed esclusiva destinazione del messaggio diffamatorio ad una sola persona determinata, **quando l'accesso alla casella mail sia consentito almeno ad altro soggetto**, a fini di consultazione, estrazione di copia e di stampa, e **tale accesso plurimo sia noto al mittente o, quantomeno, prevedibile secondo l'ordinaria diligenza**. Nel caso di specie, per le modalità di inoltro delle mail risultavano sussistenti tali condizione; il loro contenuto diffamatorio consisteva, poi, in **allusioni** circa la correttezza della condotta di amministratore e l'idoneità dello stesso a ricoprire la carica, intaccando in questo modo la reputazione acquisita nel contesto di riferimento rappresentato dall'opinione degli altri condomini. L'imputata non si era infatti limitata a contestare dei conteggi eseguiti dall'amministratore, ma li aveva definiti falsi. La pendenza, alla data di inoltro delle mail, di giudizio di opposizione ad ingiunzione di pagamento in ordine ai predetti conteggi **non integra l'esimente putativa dell'esercizio del diritto di critica**, in quanto la eventuale pretesa di una non debenza delle somme oggetto di ingiunzione non poteva, in ogni caso, legittimare la campagna altamente denigratoria promossa dall'imputata contro chi quelle somme aveva conteggiato.

Per approfondire: CORBETTA S., *Invio di una p.e.c. al responsabile di un ufficio pubblico contenente aspre critiche di un provvedimento amministrativo: è diffamazione aggravata?*, in *Diritto pen. e proc.* 2021, n. 3, p. 30, ss.; ID., *Quando si realizza la diffamazione commessa mediante invio di e-mail*, in *Diritto pen. e proc.*, 2019, n. 2, p. 204 ss.; PIERGALLINI C., *Diffamazione e diritto di critica*, in *Danno e responsabilità*, 2013, n.

11, p. 1117 ss.; MORONE A., *Diffamazione mediante il riferimento al genere e limiti del diritto di critica*, in *Giur. it.*, 2010, n. 12, p. 2632 ss..

[Corte di Cassazione, sez. V penale, sentenza 1° aprile 2022 \(ud. 25 gennaio 2022\), n. 12186/2022, Pres. Palla–Rel. Sessa](#)

6. Plurimi messaggi diffamatori su gruppo Facebook

Trascende nello scherno e nella derisione, non potendo essere scriminata dal diritto di critica, la condotta di **additare come mentalmente ipodotato** un soggetto mediante l'**invio di plurimi messaggi** all'interno di un **gruppo Facebook** con oltre duemila iscritti. La non lieve entità dell'offesa così arrecata, dato il bacino di utenza, unitamente alla sua abitudine escludono la ricorrenza, anche, della provocazione ai sensi dell'art. 599 c.p..

Per approfondire: GIACHELLO E., *La diffamazione su Facebook: un reato generazionale e un dilemma interpretativo*, in *Giur. penale*, 2018, n. 9; CORBETTA S., *Offese all'altrui onore postate su facebook: è diffamazione aggravata*, in *Diritto penale e processo*, 2016, n. 4, p. 464 ss.; DI DONNA G., *Quando la provocazione attenua la pena?* in *Rivista penale*, 2017, n. 12, p. 1075 ss.; NICOLUCCI G., *Ingiuria e diffamazione - Diffamazione - Provocazione - Limiti di operatività*, in *Giur. merito*, 2011, n. 1, p. 168 ss..

[Corte di Cassazione, sez. V penale, sentenza 5 aprile 2022 \(ud. 18 gennaio 2022\), n. 12826/2022, Pres. Pezzullo–Rel. Romano](#)

7. Molestie online e abitudine della condotta

La causa di non punibilità della particolare tenuità del fatto ex **art. 131-bis c.p. non può essere applicata**, secondo previsione testuale, ai reati necessariamente abituali ed a quelli eventualmente abituali che siano stati posti in essere mediante reiterazione della condotta tipica.

La causa di non punibilità non può dunque trovare applicazione neppure in relazione al **reato di cui all'art. 660 c.p. che in concreto abbia assunto, per il susseguirsi delle condotte moleste, l'anzidetto carattere di abitudine**, come è incontestato essere avvenuto nella specie, in cui l'imputata ripetutamente ha molestato, con il telefono e a mezzo del servizio di messaggistica istantanea *WhatsApp*, la persona offesa, inviandole immagini riproducenti momenti di condivisione intima intrattenuti con il marito di quest'ultima, legato all'imputata da relazione extraconiugale.

In senso conforme: Corte di Cassazione, sez. I penale, sentenza 8 maggio 2019 (ud. 12 giugno 2018), n. 19631/2019, Pres. Mazzei - Rel. Vannucci. (B.P.)

[Corte di Cassazione, sez. I penale, sentenza 1° aprile 2022 \(ud. 21 gennaio 2022\), n. 12013/2022, Pres. Siani - Rel. Centofanti](#)

8. Truffa online e circostanza aggravante della minorata difesa

Sussiste l'**aggravante della minorata difesa** ai sensi dell'art. 61, n. 5) c.p., nell'ipotesi di truffa commessa attraverso la vendita di prodotti online, **qualora l'autore del fatto abbia approfittato della distanza e delle particolari modalità di vendita previste dalle piattaforme online**, poiché, in tale caso, la distanza tra il luogo ove si trova la vittima, che di norma paga in anticipo il prezzo del bene venduto, e quello in cui, invece, si trova l'agente, determina una posizione di forza e di maggior favore di quest'ultimo, consentendogli di schermare la sua identità, di non sottoporre il prodotto venduto ad alcun efficace controllo preventivo da parte dell'acquirente e di sottrarsi agevolmente alle conseguenze della propria condotta, vantaggi di cui non potrebbe giovare ove la vendita avvenisse nel mondo reale.

In senso conforme: Corte di Cassazione, sez. VI penale, sentenza 10 aprile 2017 (ud. 22 marzo 2017), n. 17937/2017, Pres. Rotundo – Rel. Criscuolo; Corte di Cassazione, sez. II penale, sentenza 14 ottobre 2016 (ud. 29 settembre 2016), n. 43706/2016, Pres. Gallo – Rel. Sgadari.

Per approfondire: LEPERA M., *Un caso di reato semplice scambiato per reato circostanziato: sull'improbabile configurabilità dell'aggravante della "minorata difesa" in relazione alle truffe on-line*, in *Cass. Pen.*, 2017, n. 2, p. 687 ss.; CAJANI F., *Le truffe on line*, in PARODI C. (a cura di), *Diritto penale dell'impresa*, Milano, 2017, p. 573 ss.; PECORELLA C.-DOVA M., *Profili penali delle truffe on line*, in *Arch. Pen.*, 2013, n. 3, p. 799 ss.; CIPOLLA P., *E-commerce e truffa*, in *Giur. merito*, 2013, n. 3, p. 2624 ss..

[Corte di Cassazione, sez. II penale, sentenza 6 maggio 2022 \(ud. 13 aprile 2022\), n. 18252/2022, Pres. Rago - Rel. Nicastro](#)

9. Vilipendio commesso su Facebook

Commette reato di **vilipendio** ai sensi del codice penale militare il Sergente dell'Esercito che **commenta su Facebook** la notizia relativa all'imminente visita del Ministro dell'Interno scrivendo insulti diretti a quest'ultimo e concludendo la sua invettiva contro i "giudici comunisti", poiché tali parole unitariamente considerate tradiscono **denigrazione e totale disprezzo per la funzione pubblica rappresentata dal Governo e dalla Magistratura** e si risolvono in **mero insulto**, capace solo di deprimere la fiducia pubblica nei confronti delle istituzioni ed idonee a lederne quel prestigio che, proprio per il corretto funzionamento dell'ordinamento democratico, deve esser loro riconosciuto e garantito.

In senso conforme: Corte di Cassazione, sez. I penale, sentenza 13 agosto 2019 (ud. 15 gennaio 2019), n. 35988/2019, Pres. Di Tomassi - Rel. Mancuso.

[Corte di Cassazione, sez. I penale, sentenza 21 aprile 2022 \(ud. 23 novembre 2021\), n. 15555/2022, Pres. Santalucia – Rel. Cappuccio](#)

10. Atti persecutori e destinatario dei messaggi

Integra il reato di **atti persecutori ex art. 612-bis c.p. nei confronti** della moglie, la condotta di colui che invia svariati messaggi scritti e vocali, di minacce ed invettive **indirizzati al cellulare del figlio** della coppia, poiché tale comportamento è certamente **idoneo a raggiungere la moglie** e a causare nella stessa un grave e perdurante stato di ansia o di paura.

[Corte di Cassazione, sez. V penale, sentenza 18 maggio 2022 \(ud. 27 aprile 2022\), n. 19531/2022, Pres. Sabeone - Rel. De Marzo](#)

11. Pornografia "domestica" e "utilizzo" del minore

La Cassazione, richiamando l'arresto delle **Sezioni Unite in materia di "pornografia domestica"**, che ha individuato il discrimine tra il penalmente rilevante e il penalmente irrilevante non nel consenso del minore in quanto tale, ma nella configurabilità della sua "utilizzo" da parte del soggetto attivo, ha confermato la sentenza di secondo grado che aveva condannato l'imputato per il delitto di cui all'art. 600-ter c. 1 c.p.. Nel caso di specie, l'individuazione della "**utilizzo**" della **minore** risiedeva nell'intento dell'imputato di esaltare, attraverso le riprese, le proprie capacità erotiche, seppure apparentemente volta a valorizzare ciò che parrebbe essere solo un elemento attinente a profili soggettivo-finalistici, risolvendosi, al contempo, e simmetricamente, in una **oggettiva "mortificazione" e strumentalizzazione della persona del minore**. Il rapporto interpersonale che accompagnava le riprese era infatti un rapporto iniziato con riprese effettuate dall'imputato all'insaputa della ragazza, proseguite con la promessa, da questo mai mantenuta, di cancellarle, e terminate, addirittura, nella minaccia di diffonderle ove la ragazza non si prestasse a proseguire nella relazione.

In senso conforme: Corte di Cassazione., sez. un., sentenza 10 febbraio 2022 (ud. 28 ottobre 2021), n. 4616/2022, Pres. Cassano – Rel. Sarno.

Per approfondire: PICOTTI L., *Il ristretto ambito di non punibilità della c.d. pedopornografia domestica e l'inefficacia del consenso del minore alla diffusione di materiale pornografico con lui realizzato*, in *Diritto di Internet*, 2022, n. 3, p. 585 ss.; e già ID., *La pedopornografia nel Cyberspace: un opportuno adeguamento*

della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale riflessi nell'evoluzione normativa, in *Diritto di Internet*, 2019, n. 1, p. 177 ss. (B.P.)

Corte di Cassazione, sez. III penale, sentenza 23 maggio 2022 (ud. 14 febbraio 2022), n. 20048/2022, Pres. Marini - Rel. Andreazza

12. E' pornografia minorile utilizzare profili falsi di agenzie di modelle per ottenere foto

Integra il reato di cui all'art. 600-ter c.p., e non i reati di cui agli art. 609- *undecies* c.p. o 600- *quater* c.p., la condotta di chi, mediante l'uso di **profili falsi** e presentandosi quale responsabile di agenzie di modelle, **otteneva con l'inganno foto di ragazze nude**. Ai fini del delitto di pornografia minorile è, infatti, sufficiente anche solo **istigare o indurre il minore a produrre materiale pornografico**, trattandosi comunque di una forma di manifestazione della sua "utilizzazione" per attività vietata, la quale **non è**, peraltro, esclusa **dalla eventuale familiarità del minore alla divulgazione di proprie immagini erotiche e non richiede** nemmeno l'accertamento del **concreto pericolo di diffusione del materiale** così ottenuto.

Per approfondire: GARUTI G., *Pornografia minorile (art.600-ter c.p.) e consenso del minore*, in *Diritto pen. e proc.*, 2022, n. 4, p. 465 ss.; TACCARDI C., *La Cassazione di fronte al difficile inquadramento normativo del sexting (secondario) a cavallo tra le norme in materia di pornografia minorile e la nuova fattispecie di diffusione illecita di immagini e video sessualmente espliciti*, in *Rivista it. di medicina legale e del diritto in campo sanitario*, 2020, n. 3, p. 1621 ss.; PICOTTI L., *Il ristretto ambito di non punibilità della c.d. pedopornografia domestica e l'inefficacia del consenso del minore alla diffusione di materiale pornografico con lui realizzato*, in *Diritto di Internet*, 2022, n. 3, p. 585 ss.; ID., *Online child pornography offences- A brief overview*, in *Kriminologie und Kriminalpolitik im Dienste der Menschenwürde - Festschrift fuer Frieder Dunkel*, Verlag Godesberg, GmbH, 2020, p. 207 ss.; ID., *La pedopornografia nel Cyberspace: un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale riflessi nell'evoluzione normativa*, in *Diritto di Internet*, 2019, n. 1, p. 177 ss.; DI GIOVINE O., *La Cassazione torna sul concetto di pornografia minorile: ma è possibile interpretare un testo senza contesto?*, in *Giur. it.*, 2020, n. 6, p. 1481 ss.

Corte di Cassazione, sez. III penale, sentenza 26 maggio 2022 (ud. 8 febbraio 2022), n. 20552/2022, Pres. Ramacci- Rel. Socci

13. Il reato di indebito utilizzo strumenti di pagamento

Il reato di **indebito utilizzo di carte di credito** o di pagamento di cui all'art. 493-ter c.p., si configura anche qualora l'imputato **si limiti ad utilizzare i relativi codici, non essendo necessario il materiale possesso del documento cartaceo o plastificato**, costituendo quest'ultimo esclusivamente lo strumento che incorpora le sequenze identificative del titolare del rapporto negoziale, abilitandolo a regolare per tal via le proprie transazioni.

La fattispecie in esame, pertanto, è **pienamente integrata anche a fronte della smaterializzazione della condotta**, il cui disvalore rimane integro pur se la stessa risulta svincolata dalla disponibilità del supporto fisico. Infatti, l'espressione "indebito utilizzo" di cui all'art. 493-ter c.p., che definisce il comportamento illecito sanzionato, individua la lesione del diritto incorporato nel documento, prescindendo dal possesso materiale della carta che lo veicola e si realizza con l'uso non autorizzato dei codici personali.

In senso conforme: Corte di Cassazione, sez. II penale, 20 settembre 2019 (ud. 25 giugno 2019), n. 38837/2019, Pres. De Crescenzo – Rel. Imperiali; Corte di Cassazione, sez. II penale, sentenza 19 novembre 2014 (ud. 7 novembre 2014), n. 47725/2014, Pres. Fiandanese – Rel. Alma.

Corte di Cassazione, sez. II penale , sentenza 6 giugno 2022 (ud. 9 febbraio 2022), n. 21771/2022, Pres. Rago – Rel Pacilli

14. La peculiarità delle truffe online e il requisito degli artifici e raggiri

La **vendita online** è caratterizzata dal fatto che **essa si fonda sull'affidamento del compratore nella serietà dell'offerta** del venditore che viene pubblicizzata esclusivamente attraverso un portale *internet*. Tale particolare caratteristica delle vendite *online* determina **la natura di artificio e raggirio (ai sensi dell'art. 640 c.p.) della messa in vendita di un oggetto ad un prezzo, comunque, appetibile per il mercato e senza che la successiva mancata consegna sia dovuta a specifici fattori** successivamente intervenuti ed adeguatamente esposti dal venditore ove lo stesso ometta anche la dovuta restituzione del prezzo. Tale condotta, infatti, stigmatizza la presenza del **dolo iniziale di truffa** poiché manifesta chiaramente l'assenza di reale volontà di procedere alla vendita da parte del soggetto che, incamerato il prezzo, ometta la consegna, rifiuti la restituzione della somma ed, altresì, ometta di indicare qualsiasi circostanza giustificativa di tale (doloso) comportamento. Inoltre, sotto il profilo oggettivo, **gli artifici e raggiri vanno individuati nella registrazione presso un portale di vendite online**, nella pubblicazione dell'annuncio unito alla descrizione del bene, nella indicazione di un prezzo conveniente ovvero comunque appetibile, tutti fattori tesi a carpire la buona fede dell'acquirente ed a trarre in inganno il medesimo.

[Corte di Cassazione, sez. II pen., sentenza 15 giugno 2022 \(ud. 30 marzo 2022\), n. 23323/2022, Pres. Imperiali - Rel. Di Pisa](#)

15. I limiti della “pornografia domestica” in relazione all’età del consenso sessuale

Non può integrarsi un’ipotesi di “**pornografia domestica**” nel caso in cui il **minore** che produce ed invia il materiale pedopornografico abbia **meno di 14 anni**, non avendo raggiunto l’età per esprimere un valido consenso sessuale.

L’imputato, responsabile del reato di cui all'art. 600-*quater* c.p. per aver indotto una ragazza dell'età di tredici anni a scattarsi fotografie che la ritraevano in posizioni scabrose e ad inviargliele sul proprio profilo Facebook, contestava l’insussistenza dell’“utilizzo” della minore, non essendogli attribuibile nessun contributo causale (né in termini di costrizione né di induzione) in relazione alla produzione di detto materiale, che ha conservato ad esclusivo uso privato senza diffonderlo su altre reti o verso soggetti terzi.

Richiamandosi alla **recente evoluzione giurisprudenziale** sviluppatasi in riferimento al reato di pornografia minorile, volta a temperare la rilevanza della condotta tipica con la cd. pornografia domestica, ossia la condotta di chi realizza materiale pornografico in cui sono coinvolti minori che abbiano raggiunto l'età del consenso sessuale nei casi in cui tale materiale sia prodotto e posseduto con il consenso di tali minori e unicamente a uso privato delle persone coinvolte, al fine di **evitare ipercriminalizzazioni**, la Corte ribadisce che, al fine di circoscrivere l'area della penale rilevanza del fatto, occorre **focalizzarsi non già sul consenso del minore ma sulla configurabilità di una sua “utilizzo”** che ricorre, al momento della produzione del materiale pornografico, o per la **posizione di supremazia** rivestita dal soggetto agente nei confronti del minore, o per le **modalità con le quali il materiale pornografico viene prodotto** quali, minaccia, violenza, induzione o inganno, o per **l’età dei minori coinvolti**, qualora questa sia inferiore a quella del consenso sessuale.

La condizione che la vittima non avesse raggiunto i quattordici anni al momento del fatto (circostanza nota all’imputato) esclude la necessità di ogni indagine sull'attività manipolatoria o induttiva dell'imputato essendo sufficiente ad integrare il perfezionamento della fattispecie criminosa l'età della vittima, inferiore a quella prevista per il consenso sessuale.

In senso conforme: Corte di Cassazione, sez. un., sentenza 10 febbraio 2022 (ud. 28 ottobre 2021), n. 4616/2022 - Pres. Cassano, rel. Sarno; Corte di Cassazione, sez. un. penali, sentenza 15 novembre 2018 (ud. 31 maggio 2018), n. 51815/2018, Pres. Carcano – Rel. Andronio; Corte di Cassazione, sez. III penale, sentenza 12 febbraio 2020 (ud. 21 novembre 2019) n. 5522/2020 - Pres. Izzo, Rel. Macrì; sez. 3, 6 ottobre 2021 (ud. 11/06/2021) n. 36198/2021 - Pres. Rosi, Rel. Reynaud.

Per approfondire: PICOTTI L., *Il ristretto ambito di non punibilità della c.d. pedopornografia domestica e l'inefficacia del consenso del minore alla diffusione di materiale pornografico con lui realizzato*, in *Diritto di Internet*, 2022, n. 3, p. 585 ss.; BERNARDI S., [Le Sezioni unite chiariscono i limiti della \(ir\)rilevanza della “pedopornografia domestica” ai sensi dell’art. 600-ter c.p.](#), in SP, 25 febbraio 2022; ROSANI D., [L'introduzione giurisprudenziale di una clausola di non punibilità per la “pornografia minorile domestica”:](#) *pensieri critici*, in SP, 15 aprile 2022; SALVADORI I., *Sexting, minori e diritto penale*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Torino, 2019, p. 567 ss. (B.P.)

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

ACCINNI G.P., *L'utilizzo criminogeno della blockchain: gli smart contract*, 15 giugno 2022

BECCARI P., *Le prime difficoltà applicative della nuova fattispecie di “revenge porn” in caso di diffusione del materiale da parte di soggetti estranei al rapporto sessuale*, 7 Giugno 2022

BRAMBILLA P., *Il reato di intermediazione illecita e sfruttamento lavorativo al banco di prova della prassi: spunti di riflessione sui confini applicativi della fattispecie alla luce della prima condanna per caporalato digitale nel caso Uber*, 31 marzo 2022

CANANZI F., *Dall'emergenza alla legge delega al Governo: verso un processo penale veramente telematico?*, 21 marzo 2022

DEI-CAS E.A.A., *La partecipazione a distanza, in attesa della riforma del processo penale*, 7 aprile 2022

FRAGASSO B., *Like su Facebook ed hate crimes: note a margine di una recente sentenza della Cassazione*, 20 maggio 2022

FROVA G., *La Cassazione sulla riconducibilità all'art. 266 c.p.p. degli screenshot tramite captatore informatico*, 2 giugno 2022

MATTARELLA A., *La futura Convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica*, 11 marzo 2022

ROSANI D., *L'introduzione giurisprudenziale di una clausola di non punibilità per la “pornografia minorile domestica”: pensieri critici*, 15 aprile 2022

Diritto di Internet

MALACARNE A., *Il trojan horse “a cavallo” tra perquisizione ed intercettazione: il problema del c.d. screenshot di file multimediali*, in *Dir. Di Internet*, 2022, n. 3, p. 592 ss.

PELUSO F., CASERTA N., *Il reato di molestie o disturbo alle persone alla luce dell'innovazione tecnologica*, in *Dir. di Internet*, 2022, n. 2, p. 351 ss.

PICOTTI L., *Il ristretto ambito di non punibilità della c.d. pedopornografia domestica e l'inefficacia del consenso del minore alla diffusione di materiale pornografico con lui realizzato*, in *Dir. di Internet*, 2022, n. 3, p. 585 ss.

PITTAU F., *Sostituzione di persona e diffamazione online: i confini incerti dello stalking*, in *Dir. Di Internet*, 2022, n. 3, p. 605 ss.

SOANA G., *Autoriciclaggio mediante acquisto di cripto valute*, in *Dir. di Internet*, 2022, n. 2, p. 317 ss.

Altre riviste e contributi

AMISANO M., *Prevedere -e non predire- attraverso gli algoritmi e le loro insidie*, in *Arch. Pen.*, 2022, n. 2

BIRITTERI E., *Punire la disinformazione: il ruolo del diritto penale e delle misure di moderazione dei contenuti delle piattaforme tra pubblico e privato*, in *Riv. Trim. Dir. Pen. Cont.*, 2021, n. 4, p. 304 ss.

CRESCIOLI C., *Le recenti modifiche ai reati cibernetici, tra tardivo recepimento delle direttive europee e nuove incriminazioni: riflessioni critiche*, in *Arch. Pen.*, 2022, n. 2

D'AGOSTINO L., *Disinformazione e responsabilità delle piattaforme. Obblighi di attivazione e misure di compliance*, in *Riv. Trim. Dir. Pen. Cont.*, 2021, n. 4, p. 284 ss.

- GALIMBERTI M., *La disinformazione: profili regolatori e policy*, in *Riv. Trim. Dir. Pen. Cont.*, 2021, n. 4, p. 253
- GIUCA M., *Disciplinare l'intelligenza artificiale. La riforma francese sulla responsabilità penale da uso di auto a guida autonoma*, in *Arch. Pen.*, 2022, n. 2
- LAMANNUZZI M., *Accesso abusivo ad un sistema informatico o telematico: prospettive di riforma*, in *Arch. Pen.*, 2022, n. 1
- MAESTRI E., *Giustizia digitale Tecnologia giudiziaria e accesso alla giustizia nell'era della digitalizzazione*, in *Arch. Pen.*, 2022, n. 2
- MORGANTE G., FIORINELLI G., *Promesse e rischi della compliance penale digitalizzata*, in *Arch. Pen.*, 2022, n. 2
- PAULESU P., *Intelligenza artificiale e giustizia penale. Una lettura attraverso i principi*, in *Arch. Pen.*, 2022, n. 1
- RECCIA E., *La tipicità delle più recenti tipologie di frodi informatiche: necessità di un ripensamento? Un focus sull'attività bancaria*, in *Arch. Pen.*, 2022, n. 2
- SAMBUCO G., *Note in tema di data retention*, in *Arch. Pen.*, 2022, n. 2