News ottobre 2020

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

NOVITÀ SOVRANAZIONALI

1. Riconoscimento facciale e diritti fondamentali

L'*European Union Agency for Fundamental Rights* (FRA) ha pubblicato un *paper* che analizza le ripercussioni che hanno sulla tutela dei diritti fondamentali le nuove tecnologie di riconoscimento facciale – che trattano dati sensibili quali i dati biometrici – implementate ed utilizzate dalle pubbliche autorità. Queste nuove tecnologie sono infatti già utilizzate nel settore privato, per la pubblicità, il *marketing* e altri scopi; ad esempio, attraverso la profilazione dei singoli clienti si è in grado di prevedere le preferenze verso i prodotti in base alle espressioni facciali. Ma le tecnologie di riconoscimento facciale aprono nuove possibilità anche per la pubblica amministrazione, ed in particolare per le attività di *law enforcement* e di gestione delle frontiere. Ed è su queste ultime che si concentra il *paper* della FRA, il quale prende in considerazione, in particolare, il confronto dei filmati ottenuti da videocamere (CCTV) con le banche dati di immagini facciali (ad esempio *watchlist*) nell'ambito delle attività sopra evidenziate. Questa tecnologia, spesso definita come "tecnologia di riconoscimento facciale dal vivo", coincide con una forma specifica di videosorveglianza ed è, ad oggi, utilizzata da non molte autorità nazionali di polizia in Europa.

I diritti fondamentali che risultano maggiormente toccati dall'utilizzo di questi nuovi strumenti tecnologici sono: il diritto al rispetto della vita privata e alla protezione dei dati personali (artt. 7 e 8 della Carta di Nizza e art. 8 della CEDU); il diritto alla non discriminazione (art. 21 della Carta di Nizza e art. 14 della CEDU); i diritti dei minori (art. 24 Carta) e degli anziani; il diritto alla libertà di espressione, di riunione e di associazione (art. 11 della Carta di Nizza e art. 10 della CEDU); il diritto ad una buona amministrazione (principio del diritto dell'UE elaborato dalla CGUE e diritto fondamentale sancito dall'articolo 41 della Carta, anche se solo per le azioni delle istituzioni, degli organi e delle agenzie dell'UE); il diritto ad un giusto processo (art. 47 della Carta ed art. 6 CEDU).

Per approfondire: E. SACCHETTO, Face to face*: il complesso rapporto tra* automated facial recognition technology *e processo penale*, in Legislazione penale, 16 ottobre 2020.

Facial recognition technology: fundamental rights considerations in the context of law enforcement

2. Pubblicata la Relazione del Consiglio d'Europa sulle soluzioni digitali per la lotta al COVID-19

Nell'ottobre 2020 è stato pubblicato a cura del Consiglio d'Europa il *Report* sulla protezione dei dati 2020. La prima parte si focalizza sui provvedimenti legislativi adottati per il contrasto della pandemia da Covid-19 e analizza il loro impatto sui diritti fondamentali alla vita privata e alla protezione dei dati. In particolare, si evidenzia che gli approcci principali sono stati tre, ovvero: l'adozione di misure generali emergenziali volte a conferire al Governo poteri speciali, l'adozione di misure emergenziali in specifici settori quali la salute pubblica e l'adozione di misure d'emergenza prive di specifica base legislativa. Inoltre, si sottolinea che i principi fondamentali che devono essere salvaguardati durante lo stato di emergenza sono: principio generale dello Stato di diritto, necessità, proporzionalità, temporaneità, controllo effettivo parlamentare e giudiziario, prevedibilità, leale cooperazione tra le istituzioni statali. Il Consiglio evidenzia che misure quali quarantene obbligatorie e blocchi che limitano la libertà di movimento possono essere necessarie per combattere il Covid-19, ma non sempre rispettano i principi sopra indicati. Alcuni paesi hanno invocato la base giuridica dell'interesse pubblico alla salute per introdurre le scansioni della temperatura obbligatorie presso frontiere, aeroporti e luoghi pubblici o la registrazione obbligatoria dei dati di contatto per le visite a bar e ristoranti ai fini del tracciamento dei contatti. Tuttavia, il Consiglio evidenzia che per invocare con successo questa base giuridica, il paese deve garantire che il trattamento sia strettamente necessario a tale scopo. In particolare, l'utilizzo dei dati delle telecomunicazioni richiede un'attenzione specifica, perché i dati delle telecomunicazioni non sono solo protetti dalla normativa generale sulla protezione dei dati, ma anche da normative specifiche che garantiscono la riservatezza delle comunicazioni. Per questo motivo anche il

trattamento di dati aggregati e quindi anonimi richiede una legislazione dettagliata, poiché la creazione di tali statistiche richiede un intervento degli operatori di telecomunicazioni per il trattamento dei dati di localizzazione individuale ovvero per una finalità che non fa parte della loro competenza iniziale. In considerazione dei rischi per la protezione dei dati per le persone, i paesi non possono semplicemente fare affidamento sul motivo dell'interesse pubblico senza una legislazione specifica. Peraltro, in stato di emergenza si verificano situazioni i cui effetti non sono prevedibili e quindi risulta difficile stabilire la proporzionalità dei rimedi assunti, per cui il bilanciamento tra salute e privacy deve tenere in considerazione l'imprevedibilità degli esiti della misura adottata. Si evidenzia che in ogni caso la reale efficacia di molte misure deve ancora essere testata ed esaminata e i dibattiti sulla proporzionalità dell'interferenza con il diritto alla protezione dei dati, alla luce dell'efficacia effettiva della misura stessa, sono ancora in corso. Il Consiglio sottolinea che la trasparenza risulta essere il principio-chiave nello stato di emergenza, in quanto restituisce ai rimedi emergenziali la dignità giuridica dell'interazione con l'interessato. Trasparenza che va intesa come partecipazione alla revisione del procedimento tecnologico o algoritmico a fondamento della *app* di tracciamento oppure partecipazione alla creazione della relativa intelligenza artificiale. In tale contesto diventa necessario pubblicare il codice sorgente dell'applicazione, affinché possa essere facilmente verificato e quindi controllato, fatto che può anche aiutare a creare fiducia nel sistema, come aspetto importante della trasparenza ed a fornire strumenti di controllo del rispetto dei diritti alla privacy e alla protezione dei dati. Il Consiglio sottolinea poi che la fiducia in tali soluzioni digitali è fondamentale per il livello di adozione e quindi per l'efficacia del sistema. Gli utenti devono essere certi che il loro diritto ai dati personali sarà rispettato e la mancanza di chiarezza sullo scopo specifico, messaggi contrastanti sui motivi legali, mancata applicazione di una rigorosa minimizzazione dei dati e periodi di conservazione non fissi o molto lunghi sembrano essere tra le preoccupazioni comuni degli utenti. La seconda parte del *Report*, invece, elaborata a seguito di questionari specifici inviati ai 55 Paesi, si concentra sull'uso delle applicazioni di tracciamento digitale dei contatti e degli strumenti di monitoraggio. In particolare, emerge che le soluzioni digitali anti-Covid-19 utilizzate sono costituite essenzialmente dalle *app*, che si distinguono tra quelle a raccolta centralizzata e quelle a raccolta decentralizzata, e altri strumenti digitali, ovvero: siti *web* per fornire notizie e informazioni generali sulla pandemia, per aiutare le persone con autodiagnosi dei sintomi, per fornire istruzioni per evitare infezioni e sull'accesso ai servizi sanitari, per creare mappe per aiutare le persone a evitare gli *hotspot* dei virus, per attuare misure di contenimento, per mappare i modelli di circolazione dei cittadini, per creare statistiche giornaliere dei casi registrati, per registrare il passaggio fisico dei visitatori all'ingresso e ai punti di controllo, per consentire agli utenti di inviare segnalazioni *online* sulla violazione delle regole da parte di altre persone e per fornire il controllo della folla.

Relazione del Consiglio d'Europa sulle soluzioni digitali per la lotta al COVID-19

3. Linee Guida dell'*European Data Protection Board* sulla protezione dei dati *by design* e *by default* e l'istituzione di un *Coordinated Enforcement Framework*

Sono state adottate (e di prossima pubblicazione) dall'EDPB le linee guida sulla protezione dei dati *by design* e *by default*, le quali si concentrano sull'obbligo della protezione dei dati *by design* e *by default* per come previsto dall'art. 25 GDPR, obbligo che si sostanzia nell'effettiva attuazione dei principi di protezione dei dati e dei diritti e delle libertà delle persone interessate già nella fase di progettazione. Ciò significa che i titolari del trattamento devono prevedere misure tecniche e organizzative adeguate e le necessarie garanzie (la cui efficacia devono essere in grado di provare), volte ad attuare in pratica i principi di protezione dei dati ed a proteggere i diritti e le libertà degli interessati.

Le Linee Guida contengono indicazioni su come attuare efficacemente i principi cui all'articolo 5 GDPR, elencando gli elementi chiave di *design* e di *default*, nonché casi pratici quali esemplificazioni. Esse forniscono inoltre raccomandazioni su come i titolari, responsabili e produttori possono cooperare per adempiere all'obbligo ex art. 25 GDPR.

L' EDPB ha deciso inoltre di istituire un *Coordinated Enforcement Framework* (CEF). Il CEF fornisce una struttura per il coordinamento delle attività annuali delle autorità di vigilanza dell' EDPB. L'obiettivo del CEF è quello di facilitare, attraverso modalità flessibili e coordinate, le azioni congiunte, che vanno dallo sviluppo di una consapevolezza condivisa alla raccolta di informazioni per controlli a tappeto ed indagini. Lo scopo delle azioni annuali coordinate è quello di promuovere il rispetto delle norme, di mettere gli interessati in grado di esercitare i loro diritti e di aumentare la consapevolezza comune.

European Data Protection Board: Guidelines on Data Protection by Design and Coordinated Enforcement Framework

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Decreto immigrazione e sicurezza bis e contrasto all'utilizzo distorto del *web*

È stato approvato il d.l. 21 ottobre 2020, n. 130, c.d. decreto sicurezza bis, che tra le diverse misure contiene alcune disposizioni in materia di contrasto all'utilizzo distorto del web. In particolare, l'art. 12, rubricato "*ulteriori modalità per il contrasto al traffico di stupefacenti via internet*" prevede la formazione - da parte dell'organo del Ministero dell'interno per la sicurezza delle telecomunicazioni - un elenco costantemente aggiornato dei siti web che, sulla base di elementi oggettivi, devono ritenersi utilizzati per l'effettuazione sulla rete internet di uno o più reati di cui al T.U. stupefacenti. Tale organo deve poi provvedere all'inserimento nell'elenco ed a notificare ai fornitori di connettività alla rete *Internet* i siti *web* ai quali deve essere inibito l'accesso. A loro volta i fornitori di connettività alla rete *Internet* devono provvedere entro sette giorni a impedire l'accesso ai siti segnalati, avvalendosi degli strumenti di filtraggio e delle relative soluzioni tecnologiche conformi ai requisiti individuati dal decreto del Ministro delle comunicazioni 8 gennaio 2007. Per la violazione di tale ultimo obbligo è stata prevista una sanzione amministrativa pecuniaria. Inoltre, all'art. 9 è stato introdotto il nuovo reato di introduzione e utilizzo in carcere di dispositivi di comunicazione (art. 391-ter c.p.), che punisce chiunque procuri indebitamente o consenta ad un detenuto l'utilizzo di apparecchi telefonici o di comunicazione, o introduca in carcere i predetti.

Decreto-legge 21 ottobre 2020, n. 130

2. Decreto ristori: giustizia e Covid-19

È stato approvato il 27 ottobre 2020 il d.l. n. 137/2020, che tra le diverse misure, contiene alcune norme dedicate alla giustizia civile, penale, amministrativa e tributaria per lo svolgimento delle udienze, delle indagini preliminari e di ulteriori attività sia in ambito civile che penale in tempo di pandemia. Con riferimento al procedimento penale, l'art. 23 prevede che nel corso delle indagini preliminari il pubblico ministero e la polizia giudiziaria possano avvalersi di collegamenti da remoto per compiere atti che richiedono la partecipazione della persona sottoposta alle indagini, della persona offesa, del difensore, di consulenti, di esperti o di altre persone, salvo che il difensore della persona sottoposta alle indagini si opponga, quando l'atto richiede la sua presenza. Al co. 3 del medesimo articolo si prevede che le udienze penali per le quali è ammessa la presenza di pubblico possono celebrarsi a porte chiuse. Inoltre, si assicura, ove possibile, la partecipazione a qualsiasi udienza delle persone detenute, internate, in stato di custodia cautelare, fermate o arrestate, mediante videoconferenze o con collegamenti da remoto individuati e regolati con provvedimento del Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia. Il successivo co. 5, invece, regola lo svolgimento mediante collegamento da remoto delle udienze penali che non richiedono la partecipazione di soggetti diversi dal pubblico ministero, dalle parti private, dai rispettivi difensori e dagli ausiliari del giudice. Si prevede poi, in deroga alle disposizioni precedenti, che il giudice possa partecipare all'udienza anche da un luogo diverso dall'ufficio giudiziario. Per la decisione sui ricorsi proposti per la trattazione a norma degli articoli 127 e 614 c.p.p., invece, la Corte di cassazione procederà in Camera di consiglio senza l'intervento del procuratore generale e dei difensori delle altre parti, salvo che una delle parti private o il procuratore generale faccia richiesta di discussione orale. Infine, le deliberazioni collegiali in camera di consiglio potranno essere assunte mediante collegamenti da remoto.

L'art. 24 del d.l. n. 137/2020 disciplina l'attività di deposito di atti, documenti e istanze. In particolare, si prevede che il deposito di memorie, documenti, richieste ed istanze indicate dall'articolo 415-bis co. 3 c.p.p. presso gli uffici delle procure della repubblica presso i tribunali debba avvenire esclusivamente mediante deposito dal portale del processo penale telematico, così come gli atti indicati nel co. 2, da individuarsi tramite successivi decreti del Ministro della giustizia. Infine, il successivo co. 6 specifica che per gli atti di cui ai precedenti co. 1 e 2 non sarà consentito l'invio tramite posta elettronica certificata.

Decreto legge 28 ottobre 2020, n. 137 c.d. decreto ristori

3. Decreto del Presidente del Consiglio sul perimetro di sicurezza cibernetica nazionale

È stato pubblicato in Gazzetta Ufficiale il DPCM n. 131/2020 recante regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del d.l. 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

L'attuazione della disciplina del perimetro di sicurezza cibernetica è articolata in diverse fasi. La prima di queste è realizzata dal presente DPCM, che, fornendo previamente, all'art. 1, un elenco di definizioni (tra le più rilevanti si segnalano quelle di "pregiudizio per la sicurezza nazionale"; "incidente"; "rete, sistema informativo"; "servizio informatico", "bene ICT" ed "analisi del rischio"), provvede a fornire una definizione di: (i) le modalità e i criteri procedurali di individuazione dei soggetti (amministrazioni pubbliche, enti e operatori pubblici e privati che esercitano una funzione essenziale dello Stato o assicurano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato) inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dall'articolo 1, comma 2, lettera a) d.l. n. 105/2019; (ii) i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica *ex* art. 1, comma 2, lettera b) d.l. n. 105/2019.

Decreto del Presidente del Consiglio dei Ministri 30 luglio 2020, n. 131

Per un commento al d.l. n. 105/ 2019 conv. in legge n. 133/2019 cfr. L. PICOTTI, *Cybersecurity: quid novi?* in *Dir. Internet*, 2020, n. 1, p. 11 ss.; L. PICOTTI, R. M. VADALÀ, *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in *Sistema Penale,* 5 dicembre 2019.

4. Linee Guida dell'AGID sulla formazione, gestione e conservazione dei documenti informatici

Con queste linee guida si aggiornano e unificano le attuali regole tecniche emanate in base all'art. 71 del Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005 n. 82 e succ. modifiche) concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici. Le linee si articolano in diversi allegati relativi ai formati di file e riversamento; certificazione di processo; standard e specifiche tecniche; metadati; comunicazione tra aree organizzative omogenee di Documenti Amministrativi Protocollati.

Determinazione n. 407/2020 dell'Agenzia per l'Italia Digitale

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. L'attendibilità della vittima di violenza sessuale che naviga su *Internet* subito dopo il fatto

La Cassazione ha evidenziato che l'eventuale navigazione su *Internet* da parte della vittima di violenza sessuale subito dopo il fatto non influisce sulla sua credibilità, trattandosi di un *post factum* che nulla aggiunge o esclude rispetto al racconto delle violenze subìte.

Corte di Cassazione, sez. III Penale, sentenza 22 ottobre 2020 (ud. 14 settembre 2020), n. 29325, Pres. Vito Di Nicola – Rel. Donatella Galterio

2. La Cassazione sulla possibilità di impiegare il captatore informatico per intercettare conversazioni svoltesi utilizzando una rete *wi-fi* estera

Con questa sentenza la Cassazione si è espressa in merito alla possibilità di utilizzare il captatore informatico, c.d. *trojan*, per intercettare conversazioni tramite rete *wi-fi* estera sita in Canada. In particolare, ha respinto la tesi difensiva secondo cui i risultati delle captazioni delle conversazioni svoltesi all'estero non sarebbero utilizzabili in mancanza di rogatoria internazionale ex art. 729 c.p.p., evidenziando che il *trojan* era stato inoculato in Italia, su apparecchi telefonici in uso agli imputati collegati ad un gestore telefonico italiano e utilizzati sia in territorio italiano sia in territorio estero. Inoltre, ha sottolineato che il sistema di captazione non è costituito unicamente dal *trojan*, ma anche dalle piattaforme necessarie per il suo funzionamento, che ne

consentono il controllo e la gestione da remoto e che ricevono i dati inviati dal captatore, che in tal caso erano situati in Italia. Pertanto, poiché la registrazione della conversazioni tramite *wi-fi* sito in Canada ha costituito soltanto una fase intermedia di una più ampia attività di captazione iniziata ed oggetto registrazione, nella sua fase finale e conclusiva, sul territorio italiano e l'ascolto delle conversazioni è avvenuto in Italia su apparecchi collegati ad un gestore italiano e la cui captazione ha avuto origine sul territorio italiano, l'atto investigativo si considera compiuto sul territorio italiano, senza necessità di rogatoria.

Conformi: Corte di Cassazione, sez. II penale, sentenza 30 novembre 2016 (ud. 4 novembre 2016), n. 51034/2016, Pres. Giacomo Fumu, Rel. Geppino Rago

Corte di Cassazione, sez. II Penale, sentenza 22 ottobre 2020 (ud. 22 luglio 2020), n. 29362, Pres. Giovanni Verga – Rel. Fabio Di Pisa

3. Estradizione e tentativo di atti sessuali con minore

Il caso di specie riguarda una richiesta di estradizione avanzata dal Governo degli Stati Uniti d'America nei confronti dell'imputato, in relazione ad un mandato di arresto internazionale emesso dalla Corte Suprema della Contea di Walker (Georgia). All'estradando venivano contestati i reati di pornografia informatica e tentativo di molestie aggravate nei confronti di minori per avere pubblicato un annuncio su un sito internet (accessibile solo a maggiorenni) con il quale affermava di voler conoscere giovani uomini e ragazzi omosessuali (di anni ventiquattro o meno). All'annuncio effettuato *online* rispondeva un ispettore di Polizia, agendo sotto copertura e fingendo di essere un ragazzo quattordicenne; a tale contatto seguivano uno scambio epistolare con invio di documentazione fotografica e conversazioni telefoniche nelle quali l'estradando faceva esplicito riferimento al tipo di atti sessuali da compiere in vista di un incontro concordato. L'imputato poi, recatosi sul luogo indicato per l'incontro, veniva arrestato.

La Corte di Cassazione, accogliendo il primo motivo di ricorso, annulla la sentenza della Corte d'appello di Roma che, ritenendo integrato il tentativo del reato di atti sessuali con minore in ragione dell'annuncio pubblicato via internet, finalizzato ad intrattenere rapporti sessuali con giovani anche minorenni, accoglieva la richiesta di estradizione. Secondo i giudici di legittimità non può ritenersi integrata l'ipotesi delittuosa di cui agli artt. 56 e 609-*quater* c. p. dal momento che: (i) applicandosi la fattispecie prevista dall'art. 609-*quater* c. 1 n. 2 (trattandosi di minore quattordicenne), l'estradando non possiede una delle qualifiche soggettive espressamente previste dalla norma, la cui mancanza priva la fattispecie incriminatrice di uno dei suoi elementi costitutivi; (ii) l'annuncio pubblicato dall'imputato via internet era genericamente rivolto ad una pluralità di persone, non specificamente minorenni, e caratterizzato dalla manifestazione di un mero desiderio di conoscenza di "ragazzi più giovani (di ventiquattro anni o meno)", non accompagnata dalla estrinsecazione di atti materiali univocamente indirizzati alla instaurazione di rapporti sessuali con minori ovvero al loro reclutamento per le medesime finalità.

Non potrebbe dunque accogliersi la richiesta di estradizione poiché l'esclusione dell'ipotesi delittuosa di cui agli artt. 56 e 609-*quater* c.p. esclude al contempo la configurabilità del requisito della doppia incriminazione per l'estradizione ex art. 13 c.p. e art. II par. 1 del Trattato di estradizione tra Governo italiano e americano.

Cassazione, sez. VI penale, 16 ottobre 2020 (ud. 16 settembre 2020) sentenza n. 28814/2020 – Pres. Renato Giuseppe Bricchetti, Rel. Gaetano De Amicis

4. La Cassazione sulla differenza tra i reati di adescamento di minori e tentativo di atti sessuali con minorenne

La Suprema Corte ha ribadito che integra il tentativo del reato di atti sessuali con minorenne ex art. 609-*quater* c.p. la programmazione concreta di un incontro col minore di anni quattordici con esplicita richiesta di rapporto sessuale, trattandosi di condotta idonea ed univoca diretta al compimento di atti sessuali col minore, così come l'instaurazione col minore di un intenso rapporto telefonico di natura esclusivamente sessuale, con richieste di invio di fotografie a sfondo pornografico e proposte di incontri per consumare le pratiche sessuali oggetto delle conversazioni telefoniche, con la promessa di pagare il prezzo del viaggio in treno per raggiungere il luogo dell'incontro. Tale condotta non integra, invece, gli estremi del reato di adescamento di minori ex art. 609-*udiecies* c.p., poiché la norma in questione contiene una clausola di riserva in forza della quale il reato di

adescamento di minori si configura soltanto quando la condotta non integra gli estremi del reato-fine, ovvero l'art. 609-*quater* c.p., neanche nella forma tentata.

Conformi: Corte di Cassazione, sez. III penale, sentenza 30 luglio 2013 (ud. 11 aprile 2013), n. 32926/2013 – Pres. Claudia Squassoni, Rel. Chiara Graziosi; Corte di Cassazione, sez. III penale, sentenza 22 febbraio 2017 (ud. 29 settembre 2016), n. 8691/2016 – Pres. Aldo Finale, Rel. Giuseppe Riccardi

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

Corte di Cassazione, sez. III penale, sentenza 13 ottobre 2020 (ud. 10 settembre 2020), n. 28454/2020 – Pres. Giulio Sarno, Rel. Antonella Di Stasi

CONTRIBUTI DOTTRINALI DI RILIEVO

Diritto di Internet 4/2020

L. PICOTTI, *La violenza sessuale via* whats app

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

Sistema penale

M. GRIFFO, S*ono inutilizzabili i dati intercettati a mezzo di captatore informatico al di fuori dei luoghi consentiti*

Altre riviste

C. ROSSI, *Il reato di cui all'art. 660-*ter *c.p. è configurabile anche nel caso in cui il materiale pedopornografico sia stato realizzato dallo stesso minore. Nota a Cass. n. 5522/2020*, in *Cass. Pen.,* 2020, n. 9, p. 3245 ss.

M. TORRE, Whatsapp e *l'acquisizione processuale della messaggistica istantanea, in Dir. pen. e processo,* 2020 n. 9, p. 1279 ss.

K. NEKIT, D. KOLODIN, V. FEDOROV, *Personal Data Protection and Liability for Damage in the Field of the Internet of Things*, in 10 *Juridical Trib.*, 2020, p. 80 ss.

S. QUATTROCCOLO, *Le nuove tecnologie e il futuro del diritto pubblico*, in *Legislazione penale*, 16 ottobre 2020

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