News novembre 2020

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

NOVITÀ SOVRANAZIONALI

1. Raccomandazioni dell'*European Data Protection Board* a seguito della sentenza della CGUE sul caso Schrems II

Il 10 novembre 2020 l'*European Data Protection Board* (EDPB) ha adottato delle raccomandazioni in merito alle misure volte a garantire la sicurezza dei dati personali nei processi di trasferimento degli stessi all'interno o all'esterno dell'Unione Europea, evidenziando che vengono considerati quali trasferimenti anche l'accesso da remoto ai dati eseguito da un paese terzo e/o la conservazione dei dati in un *cloud* situato all'esterno dell'EEA *(European Economic Area*). Vengono delineati sei *step.* Tra questi, oltre al suggerimento di mappare i trasferimenti (operazione che può trovare adempimento anche grazie alla tenuta di un registro dei trattamenti *ex* art. 30 GDPR) e di identificare gli strumenti normativi *ex* art. 46 GDPR su cui si basano le proprie operazioni di trasferimento dei dati, assume particolare rilevanza il punto numero quattro, nel quale l'EDPB raccomanda di adottare misure supplementari (di cui fornisce un elenco esemplificativo nell'Allegato 2) con riguardo a tutti gli strumenti *ex* art. 46 GDPR utilizzati, nel caso in cui la legislazione del paese terzo non garantisca livelli di protezione equivalenti a quelli richiesti dal GDPR, come ad esempio nel caso degli USA, secondo quanto stabilito dalla sentenza Schrems II che ha annullato il *Privacy Schield* (cfr. Topic Privacy e precedenti News di ottobre).

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

2. Linee guida dell'ENISA per la sicurezza dell'IoT

L'Agenzia Europea per la *cybersecurity* (ENISA) ha definito delle linee guida per la sicurezza della catena di approvvigionamento dell'*Internet of Things* (IoT). Dal momento che la maggior parte di questi dispositivi è costituita da una moltitudine di componenti (sia *hardware* che *software*) provenienti da diversi fornitori, è soprattutto nella catena di approvvigionamento che devono articolarsi le basi per garantire un livello sufficiente ed adeguato di *cybersecurity*, dal momento che le organizzazioni non possono sempre controllare le misure di sicurezza adottate dai partner della catena di fornitura. Analizzando l'intera catena di approvvigionamento di prodotti e servizi dell'IoT, l'ENISA, con il contributo degli esperti del settore, ha creato delle linee guida di sicurezza per l'intero corso di vita di tali artefatti: dai requisiti e dalla progettazione, alla consegna e alla manutenzione, fino allo smaltimento finale. La sicurezza non riguarda infatti solo il prodotto compiuto, ma anche i processi per lo sviluppo del prodotto. La sicurezza dell'IoT deve essere considerata in tutte le fasi della catena di fornitura, dalla prima progettazione concettuale fino alla consegna e alla manutenzione presso l'utente finale. È quindi importante analizzare le minacce rilevanti per la sicurezza della catena logistica e, di conseguenza, definire misure di sicurezza e linee guida che aiutino ad evitare i rischi che incidono sull'affidabilità della stessa.

Guidelines for securing the Internet Of Things

3. L'adesione del *social network* TikTok all'iniziativa europea "A Safer Internet for Minors"

Anche il *social network* TikTok ha aderito all'alleanza per una migliore protezione dei minori *online*, concordando di presentare alla Commissione Europea una lista di specifici impegni e un calendario per la loro implementazione. Si tratta, in particolare, di impegni relativi a: identificare e promuovere *best practice* per la comunicazione delle informazioni relative alla *privacy* degli utenti; prevedere strumenti accessibili, robusti e semplici da utilizzare per fornire le opportune notificazioni; promuovere la consapevolezza e la responsabilizzazione degli utenti ad un corretto comportamento *online;* operare una classificazione dei contenti quando e dove risulti appropriato; promuovere la consapevolezza e l'utilizzo degli strumenti di

parental control; promuovere l'accesso dei minori a diversificati contenuti, opinioni, informazioni e conoscenze *online;* intensificare la collaborazione con organizzazioni e autorità pubbliche che si occupano della tutela della sicurezza dei minori.

TikTok commitments to an Alliance to Better Protect Minors Online

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Rapporto sull'applicazione della Legge 69/2019: un anno di "Codice Rosso"

È stato pubblicato sul sito del Ministero della Giustizia il rapporto sull'applicazione della Legge 69/2019, che ha apportato *«modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere»*. Il rapporto si prefigge di fornire un primo dato di conoscenza relativo all'applicazione della disciplina sia con riferimento ai nuovi reati introdotti, che con riguardo ai corrispondenti elementi processuali di rilievo in termini di denunce, pendenze e condanne. Tra i dati maggiormente significativi, si segnala che nel periodo compreso tra il 1° agosto 2019 e il 31 luglio 2020 risultano essere stati iscritti 1083 procedimenti per il reato di diffusione illecita di immagini o video sessualmente espliciti (art. 612-*ter* c.p.).

Con riguardo, dunque, ai nuovi reati introdotti dal Codice Rosso, sulla base dei flussi procedimentali, emerge che le nuove fattispecie rispondono ad una reale esigenza sociale se si considera l'elevato numero di procedimenti iscritti rilevati nel primo anno. In particolare, il dato corposo delle iscrizioni di notizie di reato e quello dei procedimenti già approdati alla condanna in primo grado, consentono di rilevare l'utilità concreta dell'approccio basato sull'introduzione dei nuovi reati e sulla corsia preferenziale garantita, unitamente all'ascolto della persona offesa, perché capaci di descrivere tecnicamente e di perseguire concretamente comportamenti diffusi e connotati da particolare disvalore. Il dato complessivo delle richieste di rinvio a giudizio riguardanti i nuovi reati appare significativo dell'opportunità dell'intervento normativo del cd. Codice Rosso, in mancanza del quale le gravi condotte ivi tipizzate non avrebbero avuto risposta adeguata.

Il Rapporto: un anno di "Codice Rosso"

2. Pubblicato il provvedimento che individua gli strumenti per lo svolgimento delle udienze a distanza

È stato pubblicato il provvedimento del Direttore Generale dei Sistemi Informativi Automatizzati che, in attuazione dell'art. 23, co. 2, 4, 5 e 9 del d.l. 28 ottobre 2020, n. 137, individua gli strumenti di partecipazione a distanza per lo svolgimento delle udienze civili, delle udienze penali e degli atti di indagini preliminari, nonché i sistemi telematici per le comunicazioni o notificazioni relative agli avvisi ed ai provvedimenti adottati nei procedimenti penali ai sensi dell'art. 83, commi 13, 14 e 15, d.l. n. 18/2020. In particolare, si prevedono quattro strumenti di partecipazione a distanza per lo svolgimento delle udienze penali e degli atti delle indagini preliminari. Per le comunicazioni e le notificazioni relative agli avvisi e ai provvedimenti adottati nei procedimenti penali, invece, si prevede l'utilizzo del Sistema di notificazioni e comunicazioni telematiche penali di cui alla Circolare 11 dicembre 2014, nonché del sistema ministeriale PEC TIAP-Document@ di cui ai provvedimenti DGSIA n. 1593.U del 26 gennaio 2016 e n. 19717.U del 29.9.2016. Inoltre, si assicura un collegamento riservato per il colloquio tra imputato e difensore.

Provvedimento del Direttore Generale dei Sistemi Informativi Automatizzati individua gli strumenti di partecipazione a distanza per lo svolgimento delle udienze

3. Pubblicato il provvedimento relativo al deposito telematico degli atti presso gli Uffici del Pubblico Ministero

In data 4 novembre 2020 è stato pubblicato il provvedimento del Direttore Generale dei Sistemi Informativi Automatizzati del Ministero della Giustizia, col quale è stato individuato il portale del processo telematico di cui all'art. 24, comma 1, d.l. n. 137/2020 e sono state stabilite le modalità telematiche di deposito di memorie, documenti, richieste e istanze indicate dall'articolo 415-*bis*, comma 3, c.p.p. presso gli uffici del Pubblico

Ministero. In particolare, si prevede che per il deposito degli atti di cui all'art. 1, comma 2, del presente provvedimento si debba utilizzare esclusivamente il Portale Deposito atti Penali di cui al provvedimento direttoriale n. 5477 dell'11 maggio 2020

Provvedimento del Direttore Generale dei sistemi Informativi Automatizzati del Ministero della Giustizia contenente le disposizioni relative al deposito di memorie, documenti, richieste e istanze indicate dall'articolo 415-bis co. 3 c.p.p.

4. I consigli del Garante Privacy sulla pubblicazione di immagini online e tutela della privacy

Il 24 novembre il Garante della Privacy ha diffuso un vademecum coi consigli per gli utenti che decidono di pubblicare *online* immagini o video propri o che ritraggano anche altre persone, con particolare riguardo alla gestione dei *tag* a proprio nome associati a foto o immagini. Il Garante invita principalmente gli utenti a pubblicare immagini ritraenti altre persone solo dopo aver ottenuto il loro consenso, soprattutto prima di inserire l'apposito *tag* col loro nome. Inoltre, consiglia di controllare le autorizzazioni in merito alla possibilità di accesso alle proprie immagini e di controllare i tag a proprio nome associati a foto o immagini.

Garante privacy - Consigli per tutelare la privacy

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Il momento di consumazione della frode informatica

Il delitto di frode informatica di cui all'art. 640-*ter* c.p. ha la medesima struttura ed i medesimi elementi costitutivi della truffa, dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona, di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza di quest'ultima attraverso la sua manipolazione, onde, come la truffa, si consuma nel momento e nel luogo in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui. In particolare, quando il profitto è conseguito mediante accredito su carta di pagamento ricaricabile (nella specie "Postepay"), il tempo e il luogo di consumazione del reato di truffa sono quelli in cui la persona offesa ha proceduto al versamento del denaro sulla carta, atteso che tale operazione, in ragione della sua irrevocabilità, realizza contestualmente sia l'effettivo conseguimento del bene da parte dell'agente - che ottiene l'immediata disponibilità della somma versata, e non un mero diritto di credito - sia la definitiva perdita dello stesso bene da parte della vittima.

In senso conforme: Corte di Cassazione, Sez. II Penale, sentenza 17 marzo 2020 (ud. 5 febbraio 2020) n. 10354/2020; Pres. Giovanni Diotallevi – Rel. Sandra Recchione; Corte di Cassazione, Sez. II Penale, sentenza 21 novembre 2016 (ud. 25 ottobre 2015) n. 49321/2016; Pres. Piercamillo Davigo – Rel. Cosimo D'Arrigo.

Corte di Cassazione, Sez. II Penale, sentenza 24 novembre 2020 (ud. 10 ottobre 2020), n. 32894/2020, Pres. Giovanni Diotallevi – Rel. Maria Daniela Borsellino

2. La legittimità dell'utilizzo del captatore informatico per la repressione dei reati di associazione per delinquere finalizzata al traffico di stupefacenti

La Suprema Corte ritiene legittimo l'utilizzo del cd. *virus trojan* per le intercettazioni ambientali disposte in data antecedente l'entrata in vigore del d.lgs. 29 dicembre 2017, n. 216 (cd. decreto Orlando) per la repressione dei delitti di criminalità organizzata finalizzati al traffico di stupefacenti. Infatti, evidenzia che la giurisprudenza di legittimità, in particolare con una nota sentenza delle Sezioni Unite del 2016, già da tempo ha ammesso la possibilità di utilizzare il captatore informatico per le intercettazioni ambientali, possibilità che derivava direttamente dalle disposizioni normative vigenti, in particolare dal D.L. n. 152 del 1991, art. 13, convertito in L. n. 203 del 1991, in tal modo limitandone l'utilizzo ai reati di "criminalità organizzata", come quelli elencati nell'art. 51 c.p.p., co. 3-bis e 3-quater, nonché quelli comunque facenti capo ad una associazione per delinquere, con esclusione del mero concorso di persone nel reato. L'art. 13 cit., infatti, consente per i delitti ivi elencati la captazione anche nei luoghi di privata dimora senza necessità di preventiva individuazione

ed indicazione di tali luoghi e prescindendo dalla dimostrazione che siano sedi di attività criminosa in atto, evitando in radice il problema della pervasività indiscriminata dello strumento di captazione. Inoltre, la Corte sottolinea che l'attuale testo dell'art. 266 c.p.p., non costituisce altro che la codificazione del quadro normativo preesistente così come già ricostruito dalle citate Sezioni Unite.

In senso conforme: Corte di Cassazione, Sez. Unite penali, sentenza 1 luglio 2016 (ud. 28 aprile 2016), n. 26889/2016, Pres. Giovanni Canzio – Rel. Vincenzo Romis, con nota di PICOTTI L., *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. Pen.*, n. 2, 2016, p. 1 ss. e CAJANI F., *Odissea del captatore informatico*, in *Cass. Pen.*, 2016, n. 11, p. 4140 ss.; Corte di Cassazione, Sez. Unite Civili, sentenza 15 gennaio 2020, (ud. 3 dicembre 2019), n. 741/2020, Pres. Pietro Curzio – Rel. Maria Giovanna Sambito

Per approfondire: TORRE M., *Le intercettazioni a mezzo del c.c. captatore informatico o "trojan di Stato"*, in *Cybercrime*, a cura di A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Torino, 2019, p. 1660 ss. TROGU M., *La disciplina intertemporale sull'uso del captatore informatico ai fini dell'intercettazione di comunicazioni tra presenti*, in *Proc. pen. giust.*, 2020, n. 5, p. 1243 ss.; BENE T., *"Il re è nudo": anomie disapplicative a proposito del captatore informatico*, in *Arch. pen. web*, 2019, n. 3; BONTEMPELLI M., I*l captatore informatico in attesa della riforma*, in *Dir. pen. cont.*, 20 dicembre 2018; CALAVITA O., *L'odissea del trojan horse*, in *Dir. pen. cont.*, 2018, n. 11, p. 45 ss.; GIORDANO L., *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *SP*, 2020, n. 4, p. 109 ss.; PITTIRUTI M., *L'apprensione all'estero della prova digitale*, in *Dimensione tecnologica e prova penale*, a cura di L. Lupària, L. Marafioti e G. Paolozzi, Torino, 2019, p. 205 ss.

Corte di Cassazione, sez. V Penale, sentenza 18 novembre 2020 (ud. 24 settembre 2020), n. 32426/2020, Pres. Eduardo De Gregorio – Rel. Matilde Brancaccio

3. Le questioni relative all'installazione del captatore informatico

La disposizione di un diverso decreto di autorizzazionre all'intercettazione sul medesimo bersaglio/dispositivo elettronico colpito dalle investigazioni, motivata dalla necessità di far ricorso, per ragioni investigative, allo strumento di captazione informatica sviluppato tramite virus *trojan*, configura un nuovo ed autonomo mezzo di ricerca della prova, perfettamente legittimo in presenza del rispetto dei presupposti di legge per la sua autorizzazione, che non presenta interferenze con le intercettazioni telefoniche e/o ambientali già disposte con i mezzi ordinari, pur se l'oggetto sul quale sono stati installati i captatori informatici coincide con quello su cui sono state disposte altre intercettazioni.

Inoltre, nella pronuncia i giudici di legittimità affermano che le questioni relative all'installazione del *virus trojan* per l'intercettazione in relazione all'obiettivo da intercettare non attengono alla fase autorizzativa dell'attività investigativa demandata al giudice per le indagini preliminari, né alla verifica dei presupposti di legittimità delle intercettazioni, bensì alla fase esecutiva, già coperta dall'autorizzazione a disporre le stesse intercettazioni. Fase esecutiva che è consegnata alle prerogative del pubblico ministero che può delegare la polizia giudiziaria alle operazioni materiali di installazione tecnica degli strumenti (*software*, *hardware*, *trojan*) idonee a dar vita, in concreto, alle intercettazioni; eventuali modifiche degli strumenti già indicati nel decreto autorizzativo del GIP come quelli da utilizzare per eseguire le captazioni possono essere disposte dallo stesso pubblico ministero. Le operazioni di collocazione e disinstallazione del materiale tecnico necessario per eseguire le captazioni, anche tramite *virus trojan*, costituiscono poi atti materiali rimessi alla contingente valutazione della polizia giudiziaria e l'omessa documentazione delle operazioni svolte dalla polizia giudiziaria non dà luogo ad alcuna nullità od inutilizzabilità dei risultati delle intercettazioni ambientali.

In particolare, per quanto riguarda il caso di specie, la mancata indicazione del nome dell'ausiliario che ha provveduto all'installazione del *virus* informatico per l'intercettazione è qualificabile quale omessa documentazione delle operazioni svolte dalla polizia giudiziaria delegata dal pubblico ministero all'esecuzione delle operazioni autorizzate, che non dà luogo ad inutilizzabilità o nullità dei risultati delle intercettazioni, stante l'assenza di richiamo in tal senso nell'art. 271 c.p.p., e dunque ostandovi il principio di tassatività che governa la sanzione processuale.

Corte di Cassazione, Sez. V Penale, sentenza 18 novembre 2020 (ud. 24 settembre 2020) n. 32428/2020, Pres. Eduardo De Gregorio – Rel. Matilde Brancaccio

4. L'utilizzo del captatore informatico *trojan horse* non lede la libertà morale dell'indagato

La Corte di Cassazione ribadisce che l'installazione del captatore informatico c.d. *trojan horse* non può inquadrarsi tra "i metodi o le tecniche" idonee ad influire sulla libertà di determinazione dell'indagato, come tali vietati dall'art. 188 c.p.p. Tale strumento infatti non esercita alcuna pressione sulla libertà fisica e morale della persona, né mira a manipolare o forzare un apporto dichiarativo, ma, nei rigorosi limiti in cui sono consentite le intercettazioni, capta le comunicazioni tra terze persone, nella loro genuinità e spontaneità. Inoltre, evidenzia che le Sezioni Unite nel 2016 hanno già valutato la compatibilità dell'utilizzo di tale strumento coi principi costituzionali posti a tutela della segretezza delle comunicazioni, del domicilio e della riservatezza, sottolineando che il contemperamento di valori ed interessi è già stato operato dal legislatore con l'introduzione dell'art. 13 d.l. n. 152 del 1991, che esclude espressamente per le intercettazioni tra presenti in luoghi di privata dimora disposte in procedimenti relativi a delitti di criminalità organizzata il requisito autorizzativo che il co. 2 dell'art. 266 c.p.p. richiede per tutte le altre intercettazioni.

In senso conforme: Corte di Cassazione, Sez. Unite penali, sentenza 1 luglio 2016 (ud. 28 aprile 2016), n. 26889/2016, Pres. Giovanni Canzio – Rel. Vincenzo Romis, con nota di PICOTTI L., *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. Pen*., n. 2, 2016, p. 1 ss. e CAJANI F., *Odissea del captatore informatico*, in *Cass. Pen*., 2016, n. 11, p. 4140 ss.

Per approfondire: TORRE M., *Le intercettazioni a mezzo del c.c. captatore informatico o "trojan di Stato"*, in *Cybercrime*, a cura di A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Torino, 2019, p. 1660 ss. TROGU M., *La disciplina intertemporale sull'uso del captatore informatico ai fini dell'intercettazione di comunicazioni tra presenti*, in *Proc. pen. giust.*, 2020, n. 5, p. 1243 ss.; BENE T., *"Il re è nudo": anomie disapplicative a proposito del captatore informatico*, in *Arch. pen. web*, 2019, n. 3; BONTEMPELLI M., I*l captatore informatico in attesa della riforma*, in *Dir. pen. cont.*, 20 dicembre 2018; CALAVITA O., *L'odissea del trojan horse*, in *Dir. pen. cont.*, 2018, n. 11, p. 45 ss.; GIORDANO L., *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *SP*, 2020, n. 4, p. 109 ss.; PITTIRUTI M., *L'apprensione all'estero della prova digitale*, in *Dimensione tecnologica e prova penale*, a cura di L. Lupària, L. Marafioti e G. Paolozzi, Torino, 2019, p. 205 ss.

Corte di Cassazione, sez. V Penale, sentenza 11 novembre 2020 (ud. 30 settembre 2020), n. 31604/2020, Pres. Maria Vessichelli – Rel. Elisabetta Maria Morosini

5. Reato di pornografia minorile *ex* art. 600-*ter* c.p. in caso di *sexting*

In materia di *sexting*, la Cassazione conferma l'orientamento secondo cui risponde del reato di produzione di materiale pedopornografico ex art. 600-*ter* c. 1 n. 1 c.p. colui che, pur non realizzando materialmente la condotta di produzione del materiale, trattandosi di autoscatti realizzati dal minore, abbia istigato o indotto il minore a farlo, facendo sorgere in questi il relativo proposito, prima assente, ovvero rafforzando l'intenzione già esistente, ma non ancora consolidata, in quanto tali condotte costituiscono una forma di manifestazione dell'utilizzazione del minore, che implica una strumentalizzazione del minore stesso, sebbene l'azione sia posta in essere solo da quest'ultimo.

In senso conforme: Corte di Cassazione, Sez. III Penale, sentenza 18 aprile 2019 (ud. 18 aprile 2019) n. 26862/2019, Pres. Vito Di Nicola – Rel. Stefano Corbetta.

Per approfondire: L. PICOTTI, *La pedopornografia nel* Cyberspace: *un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale*, in *Diritto di Internet*, 2019, n. 1, pp. 177-192.; I. SALVADORI, *Sexting, minori e diritto penale*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Torino, 2019, p. 567 ss.; I. SALVADORI, *I minori da vittime ad autori di reati di pedopornografia? Sui controversi profili penali del sexting*, in *Ind. pen.*, 2017, n. 3, p. 789 ss.

Corte di Cassazione, Sez. III Penale, sentenza 9 novembre 2020 (ud. 20 settembre 2020) n. 31192/2020, Pres. Giulio Sarno – Rel. Giuseppe Noviello

6. I reati di violazione della corrispondenza ed intercettazione delle comunicazioni non concorrono tra loro

In questa pronuncia la Suprema Corte ha analizzato il rapporto tra i reati di violazione di corrispondenza ex art. 616 c.p. e intercettazione delle comunicazioni di cui all'art. 617-*quarter* c.p., evidenziando che non possono concorrere tra loro in quanto i loro ambiti operativi sono differenti. Infatti, nell'ambito dell'art. 616 c.p. il termine "corrispondenza" risulta funzionale ad individuare la comunicazione nel suo profilo "statico", vale a dire il pensiero, già comunicato o da comunicare, fissato su un supporto fisico o comunque rappresentato in forma materiale, mentre nell'617-*quater* c.p. tale termine non comprende ogni forma di comunicazione, ma assume un significato più ristretto, riferibile alla comunicazione nel suo momento "dinamico", ossia in fase di trasmissione, come si ricava anche dai termini impiegati per definire la condotte alternative a quella di intercettazione, ovvero "impedisce" e "interrompe". Ne consegue che se le *mail* vengono intercettate nel momento in cui la loro trasmissione è in corso non si configura il reato di cui all'art. 616, poiché il co. 4 della medesima disposizione si riferisce alla divulgazione della corrispondenza di cui al comma 1, ossia di quella "statica".

Per approfondire v. I. SALVADORI I., *I reati contro la riservatezza informatica*, in *Cybercrime,* a cura di A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Cybercrime, Torino 2019, p. 656 ss.; L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in (ID) a cura di, *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 21 ss.

Corte di Cassazione, sez. V Penale, sentenza 4 novembre 2020 (ud.29 settembre 2020), n. 30735/2020, Pres. Carlo Zaza – Rel. Michele Romano

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*

M. GIALUZ, J. DELLA TORRE, *D.l. 28 ottobre 2020, n. 137 e processo penale: sulla "giustizia virtuale" servono maggiore cura e consapevolezza*

D. ROSANI, *Cessione di immagini pedopornografiche autoprodotte ('selfie'): la Cassazione rivede la propria lettura dell'art. 600-ter c.p.*

La legislazione penale

Speciale sulle nuove intercettazioni

F. PALMIOTTO, E. SACCHETTO, A. ROSANÒ, *Le nuove tecnologie e il futuro del diritto pubblico*, con introduzione di S. Quattrocolo

Altre riviste

A. M. RUEDA MARTÍN, *La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español*, in *Riv. trim. dir. pen. cont.*, 2020, n. 3, p. 199 ss.

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