*News dicembre 2020**

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

* Si segnala l'introduzione di un **nuovo topic**: "**FinTech**"

La scelta d'inserire un apposito topic FinTech deriva dalla consapevolezza che l'innovazione digitale nei servizi finanziari ha già raggiunto un livello di sviluppo, ma soprattutto di specificità, rispetto ai servizi finanziari tradizionali, che è destinato ad accrescersi in futuro per l'evoluzione ed espansione globale dei mercati e le esigenze di armonizzazione sovranazionale.

Quanto sopra ha un forte impatto anche sul diritto penale: il monitoraggio di questo fenomeno è funzionale a coglierne le possibili linee evolutive e le conseguenze sul piano delle eventuali manifestazioni criminali e degli interventi per prevenirli e reprimerli

NOVITÀ SOVRANAZIONALI

1. Nuova strategia dell'UE per la *cybersecurity*

Il 16 dicembre 2020 la Commissione europea e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato la nuova strategia UE per la *cybersecurity*. La Commissione, infatti, ha rilevato che le preoccupazioni relative alla sicurezza costituiscono il principale disincentivo rispetto all'utilizzo dei servizi *online*, motivo per cui è cruciale rafforzare la resilienza collettiva dell'Europa contro le minacce informatiche e contribuire a garantire che tutti i cittadini e tutte le imprese possano beneficiare appieno di servizi e strumenti digitali affidabili. La nuova strategia per la cibersicurezza mira a salvaguardare un *Internet* globale e aperto, offrendo nel contempo un meccanismo di salvaguardia, non solo per garantire la sicurezza, ma anche per proteggere i valori europei e i diritti fondamentali di tutti. Le aree di azione in cui si articola tale nuova strategia sono tre, ovvero: 1) resilienza, sovranità tecnologica e *leadership*, nella quale la Commissione propone di riformare le norme sulla sicurezza delle reti e dei sistemi informatici nell'ambito di una direttiva sulle misure dirette a garantire un elevato livello comune di cibersicurezza in tutta l'Unione al fine di aumentare il livello di cyber resilienza dei settori pubblici e privati essenziali e di avviare una rete di centri operativi per la sicurezza in tutta l'UE, alimentati dall'intelligenza artificiale; 2) costruire la capacità operativa necessaria per prevenire, dissuadere e rispondere alle minacce, intensificando la collaborazione con i partner internazionali per promuovere la sicurezza e la stabilità nel ciberspazio e proteggere i diritti umani e le libertà fondamentali online, introducendo norme e standard internazionali che riflettano questi valori fondamentali; 3) promuovere un *cyberspace* globale e aperto, aggiornando le misure esistenti a livello UE volte a proteggere i servizi e le infrastrutture essenziali dai rischi sia informatici che fisici. Per rendere efficace tale strategia nel contempo la Commissione ha presentato due proposte per rafforzare la resilienza sia informatica che fisica dei soggetti critici e delle reti essenziali, ovvero una nuova direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione (c.d. direttiva NIS 2, per sostituire quella del 2016) e una nuova direttiva sulla resilienza dei soggetti critici.

Nuova strategia dell'UE per la *cybersecurity* e nuove norme per rendere più resilienti i soggetti critici fisici e digitali

1.1. La proposta di una nuova direttiva sulle misure per un elevato livello comune di cybersecurity nell'UE (c.d. NIS 2)

La Commissione europea ha presentato una proposta di direttiva NIS 2, che andrebbe a sostituire la vigente direttiva (UE) 2016/1148, c.d. direttiva NIS (*Network and Information Security*), grazie alla quale sono stati fatti notevoli progressi nell'incremento della *cybersecurity*, ma che ha rivelato carenze intrinseche con riferimento alla crescente digitalizzazione connessa all'attuale crisi pandemica. La proposta, dunque, viene presentata allo scopo di rafforzare la protezione dei servizi e delle infrastrutture essenziali dalle minacce cibernetiche, attraverso il rinforzo della cooperazione e della condivisione di informazioni tra gli Stati membri,

la previsione di norme minime relative al funzionamento di un quadro normativo coordinato e l'introduzione di sanzioni e rimedi effettivi. In particolare, viene prevista l'estensione del campo di applicazione dell'attuale direttiva NIS ad ulteriori settori, quali servizi postali, di gestione dei rifiuti, di produzione e distribuzione di prodotti chimici, di produzione e distribuzione di prodotti alimentari e di produzione di dispositivi medici ed apparecchiature elettroniche. Inoltre, viene abrogata la precedente distinzione tra operatori di servizi essenziali (OSE) e fornitori di servizi digitali (FSD): i soggetti vengono classificati in base alla loro importanza e suddivisi rispettivamente in categorie essenziali e importanti, con sottoposizione a differenti regimi di vigilanza. Infatti, gli operatori c.d. essenziali saranno sottoposti ad un regime di vigilanza *ex ante*, mentre i soggetti importanti ad una vigilanza *ex post* in caso di inottemperanza alle disposizioni. Al fine di evitare un'applicazione disomogenea da parte degli Stati membri, la proposta prevede poi una regola generale in base alla quale tutte le medie e grandi imprese, come definite dalla raccomandazione della Commissione Europea 2003/361/CE**,** che operano nei settori o forniscono il tipo di servizi coperti dalla presente normativa, rientrano nel campo di applicazione della direttiva. Con riferimento alla gestione dei rischi, vengono rafforzati gli obblighi di sicurezza e si introduce un elenco minimo di misure di sicurezza da applicare, comprensive di controlli sulla sicurezza informatica dei propri fornitori e dell'uso della crittografia. Per quanto riguarda la procedura di segnalazione incidenti, innanzitutto viene introdotta nell'art. 4 una definizione di incidente, dopodiché si sancisce l'obbligo per ciascuno Stato membro di adottare un piano nazionale per gli incidenti di sicurezza informatica e la risposta alle crisi in cui sono definiti gli obiettivi e le modalità di gestione degli incidenti e delle crisi di sicurezza informatica su larga scala. Viene poi introdotto un rigido termine per le notifiche alle autorità competenti o al *Computer Security Incident Response Team (CSIRT)*, ovvero ventiquattr'ore dal momento dell'avvenuta conoscenza dell'incidente, con contestuale obbligo di redazione di un report finale a distanza di un mese. Per la prima volta si prevede la possibilità di ritenere le persone fisiche responsabili della violazione dei loro obblighi nel garantire l'ottemperanza alle misure di sicurezza e viene specificato che la *cybersecurity* rientra nell'ambito di responsabilità dei consigli d'amministrazione. Per rafforzare la cooperazione tra gli Stati membri viene istituita l'*European Cyber Crises Liaison Organisation Network (EU – CyCLONe)*, cui spetta il ruolo di coordinatore nella gestione degli incidenti su larga scala e di garante nello scambio regolare di informazioni tra gli Stati membri e le istituzioni europee. Il CSIRT, invece, assume il ruolo di coordinatore tra i soggetti segnalanti e i fornitori di prodotti o di servizi ICT, mentre All'*European Union Agency for Cybersecurity* (ENISA) viene affidato il compito di sviluppare e aggiornare un registro europeo per consentire agli operatori e ai loro fornitori di reti e sistemi informativi di divulgare e registrare le vulnerabilità dei prodotti o servizi ICT, nonché di fornire a tutte le parti interessate l'accesso alle informazioni ivi contenute. Infine, viene disposto un notevole incremento delle sanzioni di carattere ammimnistrativo in caso di violazione delle misure di gestione del rischio e degli obblighi di notifica.

Proposta di direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione, c.d. NIS 2

1.2. La proposta di una nuova direttiva sulla resilienza dei soggetti critici

Assieme alla proposta di adozione della direttiva NIS 2, la Commissione europea ha presentato anche un'altra proposta di nuova direttiva, dedicata alla resilienza dei soggetti critici, ovvero gli operatori che forniscono servizi essenziali per i cittadini quali strutture ospedaliere, reti energetiche, ferrovie, ma anche centri dati, amministrazioni pubbliche, laboratori di ricerca e produzione di dispositivi medici e medicinali. Tale proposta di direttiva ha come obiettivo quello di garantire che le autorità competenti designate ai sensi della presente direttiva e quelle designate ai sensi della proposta di direttiva sulla sicurezza delle reti e dell'informazione c.d. NIS 2 adottino misure complementari e si scambino informazioni, se necessario, in merito alla resilienza informatica e non e che gli enti particolarmente critici nei settori considerati essenziali ai sensi della proposta di direttiva NIS 2 siano anche soggetti a obblighi più generali di rafforzamento della resilienza per far fronte ai rischi non legati all'uso dell'energia. In particolare, si prevede l'obbligo per gli Stati membri di adottare una strategia per rafforzare la resilienza delle entità critiche, così come descritta dalla direttiva, nonché di individuare tutti gli enti che possono essere qualificato come soggetti critici, che devono adottare misure tecniche e organizzative adeguate e proporzionate per garantire la loro resilienza e notificare l'autorità competente gli incidenti che perturbano o possono perturbare in modo significativo le loro operazioni. Viene poi istituito il *Critical Entities Resilience Group*, composto da rappresentanti degli Stati membri e della Commissione, col compito di sostenere la Commissione e facilitare la cooperazione strategica e l'accesso all'informazione.

Proposta di nuova direttiva sulla resilienza dei soggetti critici

2. Report della Commissione europea sull'impatto della raccomandazione del 26 marzo 2019 sulla *cybersecurity* dei *network* 5G

Nel dicembre 2020 la Commissione europea ha pubblicato un *report* che analizza l'impatto della raccomandazione del 26 marzo 2019 in materia di *cybersecurity* dei network 5G, nonché i progressi compiuti nell'attuazione del pacchetto strumenti comune dell'UE comprendente le misure di attuazione, c.d. *EU Toolbox*. In particolare, si evidenzia che gli operatori hanno già lanciato reti commerciali 5G nelle principali città di più della metà dei Paesi membri, mentre ogni Stato membro ha effettuato una valutazione nazionale del rischio delle infrastrutture di rete 5G. Inoltre, la maggior parte degli Stati membri ha compiuto buoni progressi nell'attuazione delle misure tecniche del *Toolbox*. Si rileva che i processi nazionali sono comunque ancora in corso, ma nella maggior parte degli Stati membri sono sulla buona strada per essere completati nei prossimi mesi. Tuttavia, si evidenzia l'urgenza di ridurre il rischio di dipendenza da fornitori ad alto rischio, anche al fine di ridurre le dipendenze a livello di Unione. Infine, si rileva che gli Stati membri hanno chiesto di procedere con l'approccio coordinato dell'UE sviluppato a seguito della raccomandazione della Commissione, in particolare proseguendo il lavoro del gruppo di cooperazione NIS e di basarsi su di esso per promuovere un'ulteriore convergenza degli approcci nazionali utilizzando le strutture e i canali di cooperazione esistenti.

Report della Commissione europea sull'impatto della raccomandazione del 26 marzo 2019 sulla *cybersecurity* dei *network* 5G

3. Presentata la proposta del *Digital Service Act*

La proposta di Regolamento denominato *Digital Service Act* (DSA), che modifica la Direttiva *e-commerce* (Direttiva 2000/31/EC), compone, assieme al *Digital Markets Act* (Proposta di Regolamento europeo su mercati equi nel settore digitale), il *Digital Services Act Package*, un insieme di misure elaborate dalla Commissione Europea rivolte ai prestatori di servizi digitali offerti nell'Unione Europea con l'intento di creare uno spazio (e mercato) unico digitale più sicuro e aperto, modellato secondo principi e regole di diritto certe.
La proposta si concentra soprattutto sulla garanzia di maggiore trasparenza da parte delle piattaforme, le quali dovranno comunicare all'utente le modalità con cui vengono erogati i propri servizi e utilizzati i servizi di pubblicità, nonché sulla previsione di meccanismi di rimozione dei contenuti illeciti online. Il DSA si fonda dunque su un approccio di regolamentazione *ex ante* delle attività e dei servizi offerti dalle piattaforme online, che prevenga abusi e comportamenti illeciti o scorretti.
Il Regolamento sui servizi digitali contiene obblighi per i diversi operatori online, parametrati in base al loro ruolo, alle loro dimensioni e al loro impatto sull'ecosistema digitale. Risultano interessati dalla proposta del nuovo Regolamento: i servizi di intermediazione, che offrono infrastrutture di rete (come i fornitori di accesso a Internet) e comprendono al loro interno i servizi di *hosting* (come i servizi *cloud* e di *webhosting*), nei quali sono comprese a loro volta le piattaforme online, che riuniscono venditori e consumatori in mercati online, *app store*, piattaforme dell'economia collaborativa e piattaforme dei *social media*. In particolare, per le piattaforme online di grandi dimensioni (che raggiungono più del 10% dei 450 milioni di consumatori europei), vengono previste norme specifiche in ragione dei maggiori rischi che comportano di diffusione di contenuti illegali e di danni alla società,.
Tra le novità più significative si segnalano un meccanismo per consentire agli utenti di segnalare beni, servizi o contenuti illeciti online e alle piattaforme di collaborare con "segnalatori attendibili"; nuovi obblighi in materia di tracciabilità degli utenti commerciali nei mercati online, per contribuire a identificare i venditori di beni illegali; la possibilità per gli utenti di contestare le decisioni prese dalle piattaforme in merito alla moderazione dei contenuti; una struttura di vigilanza che rifletta la complessità dello spazio online.

Proposta di Regolamento europeo su un mercato unico per servizi digitali (c.d. Digital Services Act) che modifica la Direttiva 2000/31/EC sull'e-commerce

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. Ampliato il periodo di sperimentazione per i servizi finanziari digitali (c.d. *fintech*)

È stata pubblicata nella Gazzetta Ufficiale n. 300 del 3 dicembre 2020 la Legge 27 novembre 2020, n. 159, approvata il 25 novembre scorso dalla Camera, di conversione in legge, con modificazioni, del D.L. 7 ottobre 2020, n. 125, recante misure urgenti connesse con la proroga della dichiarazione dello stato di emergenza epidemiologica da COVID-19 e per la continuità operativa del sistema di allerta COVID, nonché per l'attuazione della direttiva (UE) 2020/739 del 3 giugno 2020. La legge di conversione ha aggiunto all'art. 1 del citato decreto un inedito co. 4-*undecies*, che, in considerazione della crescente diffusione dell'accesso ai servizi finanziari in modalità digitale da parte di cittadini e imprese durante l'emergenza epidemiologica da COVID-19, prevede nuove disposizioni in materia di servizi finanziari. In particolare, modifica l'art. 36 del D.L. n. 34 del 2019 (cd. Decreto Crescita), convertito nella Legge n. 58 del 2019, i cui commi dal 2-*bis* al 2-*decies* mirano a creare uno spazio tecnico-normativo sperimentale per le imprese del settore finanziario che operano attraverso la tecnologia (settore cd. *Fintech*), con una regolamentazione semplificata, ma garantendo un livello di protezione adeguato per gli investitori. La nuova norma del D.L. posticipa al 31 gennaio 2021 il termine per regolamentare l'avvio della sperimentazione, ne amplia la durata massima potenziale, che potrà essere prorogata per ulteriori dodici mesi, e stabilisce che i regolamenti devono definire i limiti di operatività, i casi in cui un'attività possa essere ammessa a sperimentazione e i casi in cui possa dirsi consentita una proroga. Inoltre, è stato sostituito quasi interamente il comma 2-*sexies* dell'art. 36 cit., che stabilisce ora che la Banca d'Italia, la Consob e l'Ivass, nell'ambito delle proprie competenze e delle materie seguite, adottano i provvedimenti per l'ammissione alla sperimentazione, ed ogni altra iniziativa propedeutica. Nel rispetto della normativa inderogabile dell'Unione Europea, si stabilisce poi che l'ammissione alla sperimentazione potrà comportare la deroga o la disapplicazione temporanee degli orientamenti di vigilanza o degli atti di carattere generale emanati dalle autorità di vigilanza, nonché delle norme o dei regolamenti emanati dalle medesime autorità nella specifica materia. Invece, per quanto riguarda le attività della Banca d'Italia, della Consob e dell'Ivass relative alla sperimentazione si prevede l'applicazione delle norme sulla collaborazione fra autorità e sul segreto d'ufficio. Infine, con riferimento alla possibile responsabilità civile delle autorità di vigilanza, si prevede che la colpa grave venga valutata tenendo conto anche del carattere innovativo e sperimentale dell'attività oggetto di sperimentazione.

Legge 27 novembre 2020, n. 159 di conversione in legge, con modificazioni, del D.L. 7 ottobre 2020, n. 125 con misure urgenti connesse con la proroga della dichiarazione dello stato di emergenza epidemiologica da COVID-19 e per la continuità operativa del sistema di allerta COVID, nonché per l'attuazione della direttiva (UE) 2020/739 del 3 giugno 2020

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. Il sequestro probatorio dei dispositivi informatici

Nella sentenza in esame, la Corte di Cassazione, dopo aver preso atto della divergenza di orientamenti giurisprudenziali sul punto, aderisce alla tesi per cui l'Autorità giudiziaria, al fine di esaminare un'ampia massa di dati informatici i cui contenuti sono potenzialmente rilevanti per le indagini, può disporre un sequestro dai contenuti molto estesi, provvedendo, tuttavia, nel rispetto del principio di proporzionalità ed adeguatezza, alla immediata restituzione delle cose sottoposte a vincolo, non appena sia decorso il tempo ragionevolmente necessario per gli accertamenti, senza che sia necessaria una previa perquisizione informatica. Questo perché l'effettuazione di una perquisizione informatica richiede una predisposizione di strumenti investigativi, con relativa disponibilità di tecnici, che non è compatibile con la natura di atto "a sorpresa" della perquisizione ordinaria che implica che ne siano garantite tempestività ed immediatezza, e che non può essere condizionata dalla predisposizione degli strumenti tecnici necessari per l'effettuazione di una perquisizione che richiede competenze specialistiche come quella informatica. Inoltre il codice di rito non prevede che il sequestro dei dati contenuti in supporti informatici debba essere effettuata obbligatoriamente "solo dopo" l'effettuazione della perquisizione tecnica prevista dall'art. 247 bis c.p.p. Pertanto: quando i dati contenuti in supporti informatici si configurano come "cose pertinenti al reato" per la legittimità del loro sequestro (a) deve essere

identificato il fumus del reato per cui si procede ed il collegamento tra tale reato e i dati informatici che si intendono vincolare individuando così il nesso di "pertinenza"; (b) deve essere indicata la finalità probatoria che sorregge il vincolo; (c) se non si vincolano i dati, ma l'intero supporto (o tutti i dati in modo indistinto) deve essere, altresì, identificata la ragione della necessità del sequestro "integrale", di regola riconducibile alla impossibilità di effettuare la selezione tecnica preventiva, che richiede la predisposizione di una attività tecnica e competenze specialistiche.

In senso conforme: Corte di Cassazione, sez. VI penale, Sentenza 15 dicembre 2016 (ud. 11 novembre 2016), n. 53168/2016, Pres. Giovanni Conti – Rel. Antonio Corbo.

Corte di Cassazione, sez. II penale, sentenza 31 dicembre 2020 (ud. 23 settembre 2020), n. 37941/2020, Pres. Mirella Cervadoro – Rel. Sandra Recchione

2. Il reato di diffamazione commesso tramite pec

In questa pronuncia la Suprema Corte, occupandosi di un caso di diffamazione via posta elettronica certificata, ha confermato l'orientamento secondo cui il requisito della "comunicazione con più persone" sussiste anche nell'ipotesi di invio di *e-mail* a contenuto diffamatorio direttamente ed esclusivamente destinato 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. Questo è quanto si verifica in ipotesi di trasmissione di un messaggio di posta elettronica al responsabile di un pubblico ufficio, salva l'esplicita indicazione di riservatezza. La Corte ha osservato che la casella di posta elettronica certificata non si differenzia da una normale casella di posta elettronica, se non per ciò che riguarda il meccanismo di comunicazione e la presenza delle ricevute inviate dai gestori PEC al mittente e al destinatario: il che non esclude la potenziale accessibilità a terzi, diversi dal destinatario, delle comunicazioni, attenendo la certificazione ai soli elementi estrinseci della comunicazione (data e ora di ricezione) e non già alla esclusiva conoscenza per il destinatario della e-mail originale. Tuttavia, l'utilizzazione della PEC richiede un rafforzato onere di motivazione riguardo l'elemento soggettivo del reato di diffamazione, in specie relativamente alla prevedibilità in concreto dell'accessibilità di terzi al contenuto dichiarativo. In tal senso, indici rivelatori possono essere desunti dalla conoscenza delle prassi in uso presso il destinatario, ovvero dalla natura stessa dell'atto, se destinato all'esclusiva conoscenza del medesimo o se, invece, finalizzato all'attivazione di poteri propri di quest'ultimo che, necessariamente, implichino l'accessibilità delle informazioni da parte di terzi.

In senso conforme: Corte di Cassazione, sez. V penale, sentenza 16 novembre 2012, (ud. 16 ottobre 2012), n.44980/2012, Pres. Gaetanino Zecca – Rel. Gerardo Sabeone; Corte di Cassazione, sez. V penale, sentenza 11 dicembre 2018, (ud. 22 ottobre 2018), n. 55386/2018, Pres. Antonio Settembre – Rel. Luca Pistorelli.

Per approfondire: L. Picotti, *Profili penali delle comunicazioni illecite via Internet*, in *Dir. inf. inf.*, 1999, n. 2, p. 283 ss.; G. Corrias Lucente, *Il diritto penale dei mezzi di comunicazione di massa*, Padova, 2000; G. Cassano, M. Sgroi, *La diffamazione civile e penale*, Milano, 2011; G. De Rosa, *Diffamazione tramite e-mail, aggravante del fatto commesso "col mezzo della stampa o con qualsiasi mezzo di pubblicità" ed eventuale competenza del giudice di pace: una sentenza del Tribunale di Milano*, in *Dir. pen. Cont.*, 1 marzo 2016.

Corte di Cassazione, sez. V penale, sentenza 7 dicembre 2020 (ud. 23 ottobre 2020), n. 34831/2020, Pres. Grazia Miccoli – Rel. Alessandrina Tudino

3. Atti persecutori mediante *social network*

In tema di atti persecutori *ex* art. 612 *bis* c.p. commessi nel *Cyberspace,* e più precisamente attraverso *social network,* la Corte di Cassazione ha affermato il seguente principio di diritto: la pubblicazione di post meramente canzonatori ed irridenti su una pagina *Facebook* accessibile a chiunque non integra la condotta degli atti persecutori di cui all'art. 612-*bis* c.p., mancando il requisito della invasività inevitabile connessa

all'invio di messaggi "privati" (mediante SMS, *Whatsapp*, e telefonate), e, se rientra nei limiti della legittima libertà di manifestazione del pensiero e del diritto di critica, è legittima.

Corte di Cassazione, Sez. V penale, sentenza 3 dicembre 2020 (ud. 3 novembre 2020), n. 34512/2020, Pres. Gerardo Sabeone – Rel. Giuseppe Riccardi

4. Accesso abusivo ad un sistema telematico da parte dell'*insider*

L'introduzione nel sistema informatico di uno Studio professionale da parte dell'ex socio, per effettuare il *backup* dei dati in esso inseriti, in vista dello svolgimento di una autonoma attività professionale, integra il reato di accesso abusivo ad un sistema telematico *ex* art. 615-*ter* c.p.. Seppur infatti si tratti di soggetto abilitato all'accesso in quanto dotato di *password*, ciò che rileva ai fini della realizzazione del reato è la finalità perseguita dall'agente, che deve essere confacente alla *ratio* sottesa al potere di accesso, il quale non può essere esercitato né quando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema, né quando venga mantenuto per porre in essere operazioni di natura "ontologicamente diversa" da quelle di cui sarebbe stato incaricato ed in relazione alle quali l'accesso è a lui consentito.

In senso conforme: Corte di Cassazione, Sez. Un., sentenza 8 settembre 2017 (ud. 18 maggio 2017), n. 41210/2017, Pres. Giovanni Canzio – Rel. Piero Saviani; Corte di Cassazione, Sez. Un., sentenza 7 febbraio (ud. 27 ottobre 2011), n. 4694/2011, Pres. Lupo – Rel. Fiale.

Per approfondire: I. Salvadori, *I reati contro la riservatezza informatica*, in A. Cadoppi, S. Canestrari, A. Manna e M. Papa (a cura di), *Cybercrime*, Torino, 2019, p. 656 ss.; R. Flor, *La condotta del pubblico ufficiale fra violazione della* voluntas domini*, "abuso" dei profili autorizzativi e "sviamento di poteri"*, in *Dir. Pen. Proc.*, 2018, n. 4, p. 506 ss.; R. Flor, *Verso una rivalutazione dell'art. 615-ter c.p.?* in *Riv. Trim. Dir. Pen. Cont.*, 2011, p. 126 ss.; I. Salvadori, *Quando un insider accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615-ter c.p.*, in *Riv. Trim. Dir. Pen. Economia*, 2012, p. 369 ss.

Corte di Cassazione, sez. V penale, sentenza 2 dicembre 2020 (ud. 2 ottobre 2020), n. 34296/2020, Pres. Paolo Antonio Bruno – Rel. Antonio Settembre

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

AGOSTINO L., *Art. 24 del decreto "ristori": l'interpretazione restrittiva della Cassazione in tema di deposito telematico degli atti durante il periodo emergenziale*, 2 dicembre 2020

GENNARI G., *Oscillazioni neuro...scientifiche: test a-IAT e macchina della verità*, 10 dicembre 2020

GIOSTRA G., *La nuova tutela della privacy ovvero l'assai scadente traduzione giuridica di un proponimento condivisibile*, 11 dicembre 2020

La legislazione penale

CATERINI M., *Il giudice penale robot*, 19 dicembre 2020

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