RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0087
Articolo sottoposto a peer review

Profili di contrasto al cybercrime *in iure condito* e *de iure condendo*

Vittoria Sveva Zilia Bonamini Pepoli

Nell'era del digitale la nostra vita è ormai legata a doppio filo a smartphone e tablet che ci accompagnano in ogni nostro movimento. è proprio la natura itinerante di tali mezzi che li rende perfetti "contenitori" per accogliere i c.d. captatori informatici, ovvero i malware utilizzati a fini investigativi, per il perseguimento dei reati. In questo lavoro si approfondisce come la giurisprudenza e il legislatore abbiano cercato di regolare l'avvento di questi nuovi mezzi di ricerca della prova nel tentativo di trovare un bilanciamento tra il soddisfacimento dell'interesse pubblico nell'accertamento dei reati, previsto e tutelato dall'art. 112 Cost. relativo al principio dell'obbligatorietà dell'azione penale e l'art. 15 Cost., che sancisce il principio di inviolabilità della riservatezza e segretezza di qualsiasi forma di comunicazione. Al contempo, però, si vuole sottolineare come sia essenziale il contrasto al crimine informatico, attuato anche mediante l'utilizzo di tali strumenti e un adeguato sviluppo di risorse tecnologiche per la sicurezza informatica in grado di creare sistemi che siano "cyber resilienti". In tal senso, si porta alla luce la duplice natura, benevola e malevola, dello stesso mezzo: il malware.

Malware – Cybersecurity – Cybercrime – Diritto alla riservatezza – Captatore informatico

1. Introduzione

Il concetto di "bene informatico"[1] è stato usato per la prima volta in Italia negli anni '80 del Novecento in relazione ai dati, alle informazioni e ai programmi contenuti all'interno di un apparato informatico.

A lungo la dottrina e la giurisprudenza si sono interrogate se i beni in questione fossero assimilabili, ai fini della tutela penale, ai beni di natura corporale. Il quesito nasceva, in particolare, per quel che riguardava alcuni tipi di reati quali, ad esempio, il furto o il danneggiamento.

Ebbene, la risposta a tale quesito fu negativa per via dell'impossibilità di considerare come "beni corporali" quei beni che, in realtà, non sono tangibili. Infatti, la proprietà si riferisce a beni che abbiano natura corporale essendo impossibile fare riferimento agli stessi per i beni c.d. informatici[2].

La necessità di tutelare, proteggere ma, soprattutto, regolare il bene informatico nasce da un sempre maggiore sviluppo delle reti informatiche e della conseguente diffusione dei dispositivi elettronici portatili.

Lo sviluppo ha comportato una maggiore vulnerabilità dei sistemi e delle reti così da condurre a una doppia necessità: se da un lato è fondamentale avere una serie di norme a tutela e maggiore regolazione del bene giuridico di cui sopra, dall'altro si rende indispensabile la predisposizione di misure di sicurezza finalizzate a un controllo che stimoli l'utilizzo dei sistemi informatici e una sempre maggiore «libera circolazione delle informazioni»[3].

V.S. Zilia Bonamini Pepoli è dottoranda presso la Luiss Guido Carli, nel dottorato "Diritto e Impresa". Nel corso dell'a.a. 2015/2016 ha frequentato il Master di I livello in Cybercrime e informatica forense presso La Sapienza di Roma, Facoltà di Ingegneria dell'informazione, informatica e statistica.

L'utilizzo dei sistemi informatici e, in particolar modo, dei c.d. captatori informatici quale strumento investigativo, impone un contemperamento maggiore tra la tutela del diritto alla riservatezza e le esigenze di ordine pubblico.

Dopo la sentenza Scurato[4], il Legislatore ha parzialmente regolato l'uso del captatore informatico mediante l'introduzione del d.lgs. 29 dicembre 2017, n. 216, occupandosi però di regolare solo uno degli usi del captatore informatico, quale specifica modalità di intercettazione tra presenti, avente a oggetto solo i dispositivi mobili portatili.

Nel prosieguo si analizzerà il captatore informatico e la sua natura in quanto malware che consente numerose operazioni. L'articolo è così suddiviso: il paragrafo 2 approfondisce l'anatomia e l'inserimento dei malware, soffermandosi sui captatori informatici per i dispositivi mobili; il paragrafo 3 affronta gli aspetti di natura internazionale ed europea; il paragrafo 4 analizza il tema del cybercrime *in iure condito* e *de iure condendo*. Il paragrafo 5 è dedicato alle conclusioni.

2. I malware: l'anatomia, l'inserimento e i malware per i dispositivi mobili

I malware sono software che possono apportare modifiche indesiderate o danni ai sistemi informatici. Questo termine proviene dalla contrazione di due parole inglesi: *MALicious* e *softWARE*. I malware hanno svariate funzioni: possono sottrarre le informazioni desiderate sul sistema "vittima", danneggiarle o modificarle, ma possono anche rubare le credenziali degli utenti che utilizzano il sistema; il loro scopo è quello di non creare effetti visibili sui sistemi informatici attaccati, così da poter persistere il più a lungo possibile sul dispositivo e perseguire i propri scopi.

I malware entrano all'interno dei sistemi in diversi modi: possono trovarsi nell'allegato di un messaggio e-mail[5], all'interno di un file di una pendrive USB[6] o possono trovarsi nel corso della navigazione Internet sulle pagine web visitabili[7].

Per quanto ne esistano diverse tipologie, i malware agiscono tutti nello stesso modo, possedendo un unico modello strutturale, il quale percorre quattro fasi. Una prima fase, denominata "infezione", riguarda il momento in cui il malware si introduce all'interno del sistema informatico e si installa. In questa prima fase il malware adatta alle proprie necessità le impostazioni del sistema, in particolare quella di non essere rilevato.

La seconda fase è denominata "quiescenza". Il codice del virus resta all'interno della memoria del sistema, in attesa che venga raggiunto lo scopo per cui è stato inserito. Il malware resterà all'interno del computer, finché non verrà eliminato il codice o non verrà rimosso da un software anti-malware.

La terza fase è di "replicazione e propagazione". Questa fase riguarda solo i virus e i *worm*, per i quali, al determinarsi di certe condizioni, il malware si replica e decide i bersagli da infettare, propagandosi per colpire anche altri sistemi.

Infine, la quarta fase riguarda le "azioni malevole", che corrispondono al compimento degli scopi per i quali il malware è stato inserito come la distruzione del sistema o il furto dei dati. Qualora il malware non venisse rimosso, il software tornerebbe alla fase di quiescenza.

Quando un malware entra all'interno di un sistema ha necessariamente bisogno di essere attivato dall'utente-vittima; quest'ultimo dovrà aprire il file contente il codice malevolo. Per fare in modo che la vittima non se ne accorga i file contenenti il codice sono solitamente nascosti all'interno di un contenuto lecito con struttura interna modificata. La modifica avviene attraverso la manipolazione dell'*header*, ovvero dell'intestazione di un file, contente le informazioni da mandare al sistema operativo, tra cui un puntatore che indica la prima istruzione da eseguirsi all'attivazione del programma. Quando si ha l'infezione, il virus si accoda al codice originale e dilata il file spostando il puntatore verso il codice malevolo creandone anche un altro indirizzato al codice originale. Così facendo, all'apertura del file il sistema operativo eseguirà prima il contenuto illecito e poi quello lecito.

Una volta che il malware è penetrato e ha infettato il sistema inizia una fase di quiescenza, dove il software malevolo resta in memoria finché non viene attivato. In questo momento è quiescente ma vigile per evitare di essere rilevato da parte dell'utente o di un software anti-malware.

La maggior parte dei malware, restando in memoria, possono essere rilevati da un utente esperto tramite un'applicazione che visualizzi i processi in esecuzione nel sistema operativo, motivo per cui gli attaccanti danno al software un nome di un programma già esistente all'interno del sistema; così, anche se l'utente scoprisse l'esistenza del malware non saprebbe quali tra i due programmi – quello lecito e quello illecito – eliminare[8].

Come anticipato, i controlli possono essere svolti tanto da un utente esperto, quanto da un anti-malware. Gli attaccanti sviluppano il virus in modo tale da nasconderlo anche a un eventuale programma di sicurezza; le tecniche utilizzate per smascherare il virus vengono definite "statiche" o "dinamiche".

Nel primo caso, il malware potrebbe essere rilevato attraverso la ricerca del codice malevolo all'interno di file presenti sulla memoria o su flussi di dati tra-

smessi sulla rete. Ad ogni file viene attribuita una firma, basata su algoritmi di *hash*, che lo identifica in modo univoco e perde la sua validità se il file viene modificato. Il malware verrebbe rilevato attraverso un codice virale, anch'esso codificato con algoritmi di *hash*, chiamato *virus signature*. Il programma antivirus scansiona tutti i file e rileva corrispondenze errate tra i dati e le sequenze dei codici virali note. Questo metodo sarà valido per tutti i malware che sono conosciuti, mentre nulla varrà nei confronti di quei malware non ancora noti. I produttori dei programmi antivirus aggiornano continuamente i software da loro prodotti ma, per proteggere il sistema dal giorno in cui potrebbe essere rilasciato il malware "sconosciuto" a quello in cui verrà aggiornato il database, vengono utilizzate tecniche statiche che permettono il riconoscimento del codice malevolo senza avvalersi però del sistema delle firme. La tecnica in questione prevede che vengano raccolti dapprima i dati – i quali si riferiscono ad una particolare caratteristica virale, ad esempio, la presenza di un codice cifrato – poi, verranno analizzati tramite l'associazione ad un certo grado di pericolosità e sarà stilato un report che raccoglie le statistiche con riguardo al file oggetto di scansione. Ogni valore verrà aggiunto al report e il suo contenuto verrà valutato come pulito, sospetto o infetto. Questo tipo di tecnica statica si basa sull'euristica, per via della mancata conoscenza dei malware. è evidente come dapprima sia necessario effettuare dei tentativi utili per trovare eventuali virus.

Solitamente, per nascondersi dai controlli statici anti-malware gli attaccanti mascherano il codice malevolo, così da renderlo illeggibile e mutevole nel tempo; lo stesso verrà cifrato per non essere rilevato tramite firme predefinite. La cifratura del malware – tramite l'uso di un'apposita chiave, detta *stub* – comporta, prima, che lo stesso venga decifrato. La chiave *stub* cifra e decifra il codice malevolo[9]. Tale chiave non sarà statica ma muterà di volta in volta per rendere il codice cifrato sempre diverso.

Un'altra tecnica utilizzata è quella di comprimere il codice malevolo tramite l'uso di un algoritmo di compressione. Così facendo la vittima non verrà insospettita da un'occupazione anomala della memoria. La tecnica in esame è nota come "pacchettizzazione" e prevede l'inserimento nel codice di una sequenza di istruzioni per lo spacchettamento.

Gli anti-malware utilizzano anche tecniche dinamiche per rilevare i virus: attraverso le stesse viene rilevato il comportamento dei programmi in esecuzione. Il monitoraggio è un elemento dell'antivirus, residente nella RAM, che ricerca comportamenti sospetti. Se viene rilevata un'azione allarmante il software può bloccare l'operazione corrente oppure terminare il programma o, ancora, chiedere all'utente di scegliere l'azione da intraprendere.

I malware fino a ora richiamati operano a livello locale, infettando un sistema per volta. Ebbene, esistono anche tipologie di malware che hanno come obiettivo quello di infettare a livello distribuito; così facendo ogni sistema infettato entra a far parte di una *botnet* formata da dispostivi collegati a Internet e controllati da un'unica entità, il *botmaster*.

Una *botnet* può essere composta da milioni di sistemi – detti *bot* o zombie – che possiedono un *kernel*[10] per scambiare informazioni con uno o più server remoti. Per fare questo, sfruttano i servizi di chat connettendosi a un canale protetto da una password o da reti peer-to-peer attraverso le quali controllano e impartiscono gli ordini ai sistemi infetti.

Solitamente le *botnet* vengono utilizzate per compiere attacchi "distributed denial of service" – i DDoS mirano a compromettere il funzionamento del sistema informatico attraverso l'invio di numerosi messaggi fino a esaurirne le risorse – o campagne di spam, ossia mail pubblicitarie volte a reclamizzare un prodotto.

Di seguito verranno generalmente richiamati esempi di incidenti informatici dovuti alla presenza di diverse tipologie di malware. Un primo caso è rappresentato dai *ransomware*, ovvero una particolare tipologia di malware il cui obiettivo è impedire alla vittima di accedere al sistema informatico e utilizzarne i documenti. Secondo il *2016 Italian Cybersecurity Report* di CIS Sapienza si tratta di un fenomeno in crescita. Vi sono anche i *malware Eye Pyramid*. Questo tipo di malware si diffonde tramite l'e-mail e, una volta installato, accede ai documenti e alla casella di posta elettronica del sistema infetto. Inoltre, cattura i tasti che vengono digitati dalla vittima, permettendo di captare ogni tipo di informazione.

Alla luce di quanto detto, è evidente come i malware abbiano giocato un ruolo fondamentale nell'acquisizione della prova tramite le intercettazioni effettuate sui telefoni cellulari e sui computer. I malware – denominati dalla giurisprudenza "captatori informatici" – vengono inseriti all'interno dei dispositivi mobili per acquisire le comunicazioni tanto tra presenti – le c.d. intercettazioni ambientali – quanto qualunque altro tipo di conversazione telefonica o di messaggi tra il soggetto intercettato e i terzi.

I captatori informatici vengono inseriti all'interno dello smartphone, o dei tablet, potendo cancellare o rubare i dati sensibili e potendo accedere a tutte le informazioni presenti sui sistemi infettati effettuando, ad esempio, screenshot dello schermo e acquisendo i dati presenti nella memoria e qualunque tipo di informazione, quali numeri di telefono, appuntamenti condivisi, e-mail, messaggi e geolocalizzazioni.

Tra i maggiori sistemi operativi presenti sul mercato della telefonia mobile ci sono "Google Android" e "Apple iOS", accomunati da politiche di sicurezza volte a proteggere contro accessi fisici non autorizzati, cifratura dei contenuti personali dell'utente[11] etc.

Secondo le statistiche, la maggior parte delle minacce riguarda i sistemi "Google Android" mentre una minima parte interessa i sistemi iOS, ciò è dovuto alla tipologia di sistema operativo. Il primo, infatti, è un sistema open source in cui colui che utilizza il dispositivo ne ha un pieno controllo, mentre iOS si caratterizza per avere una piattaforma chiusa dove l'utente ha molte meno possibilità di personalizzazione; questo comporta che il modello di sicurezza tra i due sistemi sopra citati è completamente diverso. *Apple* controlla, tramite l'*App Store*, ogni applicazione presente sul telefono verificando che il codice realizzato dagli sviluppatori sia legittimo[12].

L'inserimento dei malware all'interno dei dispositivi mobili viene effettuato principalmente attraverso il Web o i c.d. market (negozi di applicazioni).

Attraverso il Web, il malware si diffonde tramite un *drive-by download*[13]. Così facendo, il programma malevolo si introduce in modo silente nel sistema vittima senza che sia necessaria alcuna autorizzazione da parte della vittima.

Nel caso di market invece, viene realizzata un'applicazione apparentemente legittima che invogli l'utente a scaricarla. Alcuni esempi riguardano giochi particolarmente conosciuti. La realizzazione di questo tipo di malware è il *repackaging*, tramite cui un utente malevolo modifica e personalizza l'applicazione inserendovi il codice virale. Una volta completato il processo di "decompilazione" si avrà un'applicazione identica a quella originale che però non avrà alcuna firma digitale perché compromessa durante il processo menzionato.

La firma sarà facilmente realizzabile tramite un certificato "auto firmato", attraverso un canale non ufficiale; da questo momento l'applicazione potrà essere distribuita tramite una fonte sconosciuta. Anche se, solitamente, le impostazioni del sistema operativo non permettono che vengano installati questi contenuti, tramite una modifica da parte dell'utente l'applicazione potrà trovare ingresso all'interno del computer.

3. Gli aspetti giuridici internazionali ed europei sui reati informatici

La protezione giuridica dei sistemi informatici ha catturato l'attenzione sia del diritto nazionale sia di quello internazionale ed europeo. Il Consiglio d'Europa ha redatto una Convenzione internazionale contro la criminalità del cyberspazio[14], attraverso una lista di reati informatici e l'invito rivolto agli Stati membri di adeguare le proprie legislazioni.

Il Comitato dei Ministri adottò il progetto e lo aprì alla firma degli Stati europei ed extraeuropei in occasione della conferenza sul cybercrime tenutasi il 23 novembre 2001 a Budapest[15].

Tale Convenzione ebbe un ruolo fondamentale per il contrasto alla criminalità informatica, influenzando le legislazioni degli Stati membri del Consiglio d'Europa, al fine di regolamentare una materia che, fino ad allora, era stata oggetto unicamente della legge del mercato[16].

L'obiettivo primario della Convenzione[17] era quello di introdurre un target minimo sulla tutela dei beni giuridici offesi dai reati informatici e uno comune di strategie di contrasto per tali delitti, perseguendo l'obiettivo di creare un'armonizzazione tra le norme di contrasto presenti nei vari ordinamenti, data la natura transfrontaliera che talvolta hanno tali tipi di illeciti. A ciascuno Stato restava ferma la possibilità di disciplinare in modo più restrittivo la materia in esame[18].

In ambito europeo, con il Trattato di Lisbona la criminalità informatica è stata inserita nell'art. 83 TFUE tra i fenomeni di criminalità considerati come particolarmente gravi e di natura transnazionale, su cui l'Unione europea ha competenza penale. Con la direttiva 2016/1148[19], detta direttiva NIS[20], l'Unione europea ha inteso intensificare la sensibilizzazione degli Stati membri alla sicurezza del cyberspazio avverso la commissione dei reati informatici, attraverso l'adozione di misure volte a tutelare la sicurezza delle reti e i sistemi informativi dell'Unione europea. Gli obiettivi individuati dalla direttiva ai quali deve adeguarsi l'ordinamento nazionale degli Stati membri sono: gli obblighi di una maggiore trasparenza delle reti informatiche, tanto a livello nazionale che sovranazionale e un maggiore radicamento delle misure di sicurezza nei diritti sanciti dalla Carta dei diritti fondamentali dell'UE, a garanzia della libertà di espressione, della tutela dei dati personali e della vita privata. Inoltre, deve essere garantito un libero accesso alle reti verso tutti i cittadini dell'Unione, così da evitare qualunque analfabetismo digitale[21].

Tra gli obiettivi vengono individuate delle priorità strategiche secondo le quali è necessario raggiungere una cyber-resilienza tramite l'abbattimento del crimine informatico; sviluppare una politica comune tra gli Stati membri di "cyber-difesa" congiuntamente alla Politica di sicurezza e di difesa comune; sviluppare risorse industriali e tecnologiche per la sicurezza informatica e, infine, adottare una politica internazionale dell'UE riguardo Internet basandosi sul rispetto dei valori fondamentali dell'Unione europea. L'ultimo obiettivo posto dalla direttiva del 2016 è

quello di condividere la responsabilità per garantire la sicurezza delle reti, dovuto dalla sempre maggiore dipendenza che si ha nei confronti delle tecnologie dell'informazione e alla maggiore vulnerabilità per via dell'impatto che le reti e i sistemi informativi hanno nella vita quotidiana.

La direttiva NIS è rivolta alla protezione europea dalle minacce cyber delle infrastrutture critiche. In particolare, lo scopo della direttiva è quello di garantire una tutela di base e comune, verso le informazioni, le reti e i sistemi, all'interno dell'Unione europea, per salvaguardare la continuità dei servizi strategici in ambito civile, sociale ed economico[22].

Sempre nell'alveo della strategia europea in materia di cybersicurezza, a giugno 2019 è entrato in vigore il Regolamento UE sulla cybersicurezza[23] definita come «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche»[24]. Il Regolamento introduce un sistema europeo di certificazione e un nuovo mandato, più forte, per l'Agenzia dell'Unione europea per la cybersicurezza[25].

La strategia adottata dall'Unione europea si pone l'obiettivo di creare un cyberspazio resiliente, che sia aperto e sicuro e che porti a una maggiore fiducia da parte dei cittadini europei verso gli strumenti e i servizi digitali.

4. Il cybercrime: *in iure condito* e *de iure condendo*

Alla fine dell'800 due giovani avvocati di Boston, Samuel Warren e Louis Brandeis, partendo dallo *jus solitudinis* – ovvero *right to be let alone* – coniarono il termine giuridico privacy, riservatezza, con un saggio pubblicato nel dicembre del 1890 dalla Harvard Law Review[26].

La nozione originaria di privacy e riservatezza riproduceva lo schema del diritto alla proprietà privata che esclude gli altri, a meno che non siano legittimati a entrare. La rivoluzione digitale ha trasformato la nozione di sfera privata, riguardo alle informazioni trasmesse e ricevute, attraverso scambi sempre più immediati ma non sempre controllati.

A livello internazionale, l'art. 8 CEDU[27] afferma il diritto al rispetto della corrispondenza di ciascuno e la non ingerenza dell'autorità pubblica nell'esercizio di tale diritto. L'eccezione a tale affermazione è costituita dalla possibilità che sia la legge a prevedere un'ingerenza da parte dell'autorità pubblica per garantire la tutela e il rispetto della pubblica sicurezza, del benessere economico del paese, della difesa, dell'ordine e della prevenzione dei reati. Per proseguire nel panorama internazionale, l'art. 17 del Patto Internazionale relativo ai diritti civili e politici[28] del 1966 sostiene il divieto di interferenze nella vita privata e nella corrispondenza di ciascuno, ritenendo che sia la legge a dover tutelare tale diritto.

In ambito europeo, con la Direttiva 95/46/CE[29] venne introdotta la tutela delle persone fisiche, con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati. Successivamente, con l'entrata in vigore della Carta dei diritti fondamentali dell'Unione europea – c.d. Carta di Nizza – si riconobbe espressamente il diritto alla protezione dei dati personali. In particolare, l'art. 7 della Carta di Nizza[30] afferma il diritto al rispetto della vita privata e di quella familiare estendendo tale diritto anche alla corrispondenza. Ancora, l'art. 8 riconosce espressamente il diritto alla protezione dei dati personali[31]. Con l'entrata in vigore del Regolamento Generale sulla Protezione dei Dati (GDPR)[32] la direttiva 95/46/CE viene abrogata.

Il nuovo Regolamento raccoglie l'esperienza europea degli ultimi anni, con particolare riferimento agli approdi giurisprudenziali della Corte di Giustizia dell'Unione europea e, in particolare, alla progressiva trasformazione dell'orientamento delle istituzioni europee verso una normativa europea sulla libera circolazione dei dati personali più incentrata sulla tutela dei diritti fondamentali[33].

Nell'ordinamento italiano, il diritto alla riservatezza ha il suo primo referente nel complesso di principi ricavabili dall'art. 2 della Costituzione.

Il diritto alla riservatezza viene desunto dall'interpretazione data di alcune norme della Costituzione quali: l'art. 13 sulla libertà personale, l'art. 14 sull'inviolabilità del domicilio e l'art. 15 che garantisce il diritto all'inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione. Al secondo comma dello stesso articolo si afferma come, su disposizione motivata dell'autorità giudiziaria possa essere limitato il diritto di cui al primo comma, con le garanzie stabilite dalla legge[34].

Il diritto alla riservatezza si afferma nella giurisprudenza italiana a partire dagli anni Settanta[35] per proseguire fino alla legge 31 dicembre 1996 n. 675[36], confluita nel Codice Privacy[37], poi modificato dal decreto legislativo n. 101/2018[38].

Da una sommaria disamina della normativa menzionata, si può notare come la riservatezza sia sempre stata uno dei diritti cardine, tanto a livello nazionale quanto a livello europeo e internazionale. La sua tutela incontra come unico limite un atto motivato dell'autorità giudiziaria per garantire il rispetto di un bene, come per esempio la pubblica sicurezza, anch'esso tutelato dal legislatore.

In caso di intercettazioni a scopo investigativo attraverso l'utilizzo di un "agente intrusore", il virus informatico, c.d. trojan[39], il diritto alla riservatezza rischierebbe quindi di essere leso. Difatti, la forza invasiva del trojan porterebbe a una compressione del diritto in questione, essendo quindi necessario un bilanciamento tra le esigenze investigative e i diritti fondamentali dell'individuo.

In un primo momento, l'utilizzo dei trojan consentiva quella che era stata definita "perquisizione on line o elettronica". In tal caso, ci si riferiva all'installazione da remoto di un programma inviato congiuntamente a messaggi e-mail o sms, di un captatore informatico in un computer o in uno smartphone[40]. Tramite questo strumento è possibile captare tutto il traffico telefonico o informatico in arrivo e in partenza dal computer o dal cellulare; le informazioni che si vogliono captare sono, per così dire, "infettate" dal malware e lo smartphone diventa un mezzo controllato dal soggetto terzo che ha introdotto il captatore. Può essere attivata la videocamera, carpendo così le immagini e può essere copiata la memoria e decifrato quello che viene digitato sulla tastiera. I dati raccolti potranno così essere trasmessi in tempo reale in un sistema informatico in uso alla polizia giudiziaria.

Il sistema descritto è altamente utile per le indagini, permettendo ad esempio, che venga intercettata una comunicazione telefonica intercorrente tra due soggetti e direttamente sui loro terminali senza attraversare una struttura centrale di commutazione. In questo modo, la comunicazione viene captata per mezzo di dati informatici in forma crittografata, potendo essere letti solo da chi possiede la chiave di decodifica.

Nell'era dello smartphone, il presupposto dell'utilizzo del telefono cellulare è che tale oggetto sia sempre con noi, accompagnandoci in ogni nostro movimento e in ogni luogo. Così facendo, il legame di "dipendenza" che si crea tra il cellulare e la persona intercettata permette il suo utilizzo ovunque, quale perfetto mezzo di intercettazione (anche della vita dei terzi, che entrano in contatto con il soggetto intercettato).

In un primo momento la giurisprudenza di legittimità dichiarò infondate le censure verso i procedimenti cautelari sia per questioni di rito, riguardanti la genericità dei motivi, che per le implicazioni della normativa speciale, riguardo alle intercettazioni nei procedimenti di criminalità organizzata. In particolare, la giurisprudenza affermò che la censura relativa a un difetto di motivazione riguardante la mancata specificazione che nei luoghi di privata dimora, sottoposti a intercettazione ambientale, si stesse svolgendo l'attività criminosa risultava infondata. L'infondatezza della censura era motivata dal fatto che le captazioni erano state disposte *ex* art. 13 d.l. 13 maggio 1991, n. 152, conv. con modificazioni in l. 12 luglio 1991, n. 203 che prescinde da tale requisito, poiché prevede che l'intercettazione di comunicazione tra presenti è consentita anche se non vi è motivo di ritenere che nei luoghi indicati dall'art. 614 c.p. si stia svolgendo l'attività criminosa[41].

Di segno opposto un secondo orientamento interpretativo della giurisprudenza di legittimità che affrontò il tema del nuovo strumento investigativo attraverso una disamina delle peculiarità tecniche che contraddistinguevano tale modo di eseguire le intercettazioni: l'attivazione a distanza del microfono e quella della telecamera[42]. La Corte di Cassazione affermò che l'attivazione a distanza del microfono rappresentava un'intercettazione ambientale; la sua legittimità andava valutata alla luce dell'art. 266, comma secondo, c.p.p. e riguardava l'intercettazione di comunicazioni tra presenti in un luogo determinato. La norma doveva essere interpretata alla luce dell'art. 15 Cost. Il punto dolente era però rappresentato dalla possibilità che il soggetto si spostasse e il cellulare – attivo in qualità di microfono – captasse qualunque conversazione fatta dal soggetto intercettato con terzi, in una pluralità di luoghi diversi. Così facendo, la giurisprudenza di legittimità diede un'interpretazione costituzionalmente orientata propendendo per la tesi secondo cui le intercettazioni sono legittime solo nei luoghi specificati dal decreto autorizzativo, il quale dovrà individuare con precisione dove dovrà essere espletata l'intercettazione delle comunicazioni tra presenti, non essendo legittimo quel provvedimento autorizzativo che indica in modo indeterminato i luoghi o, addirittura, non dà indicazioni a riguardo. Il secondo aspetto problematico riguardava l'attivazione a distanza della telecamera del telefono cellulare o del computer per effettuare le video riprese. Le video riprese non possono essere effettuate ovunque per evitare violazioni dell'art. 14 Cost. La tutela costituzionale del domicilio è riservata ai luoghi con i quali il soggetto ha un rapporto stabile; nel caso in cui le attività si svolgano in luoghi che non hanno natura di domicilio, le video riprese possono essere effettuate incontrando come unico limite la tutela alla riservatezza di cui all'art. 8 CEDU e dell'art. 2 Cost. Le prove così acquisite potranno essere utilizzate in qualità di prove atipiche in quanto ammesse con un provvedimento motivato dell'Autorità giudiziaria.

A tal fine, ad avviso della Corte, non saranno utilizzabili quelle riprese effettuate tramite l'uso dell'agente intrusore all'interno del domicilio e quelle compiute in ambienti in cui vada salvaguardata la riservatezza a meno che non vi sia un provvedimento dell'Autorità giudiziaria che specifichi le ragioni che inducono a compiere l'atto per la ricerca della

prova del reato. La Corte di Cassazione dà, quindi, un'interpretazione restrittiva escludendo che le intercettazioni ambientali tramite captatore informatico possano essere attuate ovunque si sposti il soggetto, essendo ritenute legittime soltanto qualora il decreto autorizzativo individui con precisione i luoghi in cui deve essere espletata l'attività captativa[43].

Nel 2016 si ha un importante punto di svolta sull'utilizzo dei captatori informatici per le intercettazioni ambientali. In particolare, la Corte di Cassazione[44] rimette alle Sezioni Unite la questione, formulando dei quesiti, così sintetizzabili: se nei luoghi di privata dimora *ex* art. 614 c.p., anche se non precisamente individuati e senza che si stia svolgendo l'attività criminosa, sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un captatore informatico in dispositivi elettronici portatili (come per esempio personal computer, tablet, smartphone)[45]. Le Sezioni Unite della Cassazione[46] rilevarono che per i reati di cui all'art. 51, comma 3-*bis* e comma 3-*quater* c.p.p., nonché comunque facenti capo a un'associazione per delinquere con esclusione del mero concorso di persone nel reato, l'uso del virus informatico è consentito anche nei luoghi di privata dimora, per realizzare intercettazioni "tra presenti", senza necessità che sia in atto l'attività criminosa e senza una preventiva individuazione degli stessi[47].

Al di fuori dell'ipotesi della commissione di reati di criminalità organizzata, la Corte rileva che si potrà comunque procedere all'uso di trojan, purché venga richiesto *ex ante* nel provvedimento di autorizzazione e vengano ribaditi i luoghi nei quali espletare l'attività di intercettazione della/e comunicazione/i determinando così quelle da escludere, fatta salva l'attività criminosa *in itinere*.

In attuazione dei criteri contenuti nell'art. 1, comma 84, lett. e), della legge n. 103 del 2017[48] è stato adottato il d.lgs. 29 dicembre 2017, n. 216[49], che, nell'ambito della riforma delle intercettazioni ha disciplinato l'utilizzo nelle indagini del captatore informatico[50]. Alcune delle modifiche più rilevanti riguardano, in particolare, l'art. 4 del d.lgs. 216/2017, che ha modificato il codice di procedura penale in materia di intercettazioni, mediante l'inserimento del captatore informatico, fissando i limiti di ammissibilità delle intercettazioni tra presenti. Difatti, è stato modificato l'art. 266, comma 2, c.p.p. inserendo la possibilità di eseguire le intercettazioni tra presenti anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora le intercettazioni avvengano nei luoghi di privata dimora è possibile eseguirle solo qualora vi sia fondato motivo di ritenere che in quei luoghi si stia svolgendo l'attività criminosa[51].

Inoltre, è stato inserito dall'art. 4 del decreto legislativo citato anche il comma 2-*bis* per il quale l'intercettazione di comunicazioni tra presenti mediante l'uso del trojan inserito su dispositivo elettronico portatile è sempre consentito nei procedimenti per i reati di criminalità organizzata, ovvero quelli elencati nell'art. 51, commi 3-*bis* e 3-*quater*, c.p.p.[52]

Per quanto riguarda i presupposti e le forme del decreto che autorizza l'intercettazione tra presenti mediante l'utilizzo del captatore informatico, il nuovo art. 267 c.p.p. dispone che il giudice per le indagini preliminari debba autorizzare con decreto motivato quando vi siano gravi indizi di reato e l'intercettazione è considerata come assolutamente indispensabile ai fini della prosecuzione delle indagini. Inoltre, il decreto autorizzativo del gip dovrà essere adeguatamente motivato in merito alla scelta di ricorrere all'uso del captatore informatico per rilevare le conversazioni tra presenti. Al contempo, qualora si proceda per delitti diversi da quelli indicati dall'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. e dei delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione, per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, il decreto autorizzativo dovrà indicare gli ambienti e il tempo in cui la stessa dovrà avvenire[53], «secondo un verosimile progetto investigativo che implica l'individuazione anche in forma indiretta dei luoghi in cui si sposterà il dispositivo mobile controllato, e sempre che si proceda "per delitti diversi da quelli di cui all'art. 51, commi 3-*bis* e 3-*quater*"»[54]. Ancora, qualora vi siano casi di urgenza e vi sia fondato motivo di ritenere che dal ritardo possa derivare un pregiudizio grave per le indagini, il pubblico ministero procede con decreto motivato all'intercettazione tra presenti mediate l'inserimento del trojan su dispositivo elettronico portatile. Tale evenienza è possibile solo per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. e per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni. Inoltre, il pubblico ministero, oltre a indicare le ragioni che rendono necessaria tale scelta per lo svolgimento delle indagini, indica anche le ragioni dell'urgenza che non rendono possibile attendere il provvedimento del giudice[55].

La modifica stessa all'art. 267 c.p.p. mette in risalto come il ruolo svolto dal giudice per le indagini preliminari si faccia più intenso attraverso un'ingerenza diretta nelle indagini svolte dal pubblico ministero e una valutazione sull'utilità dello strumento investigativo richiesto da quest'ultimo[56].

Infine, sono state apportate delle modifiche anche in riferimento all'art. 270 c.p.p. sull'uso processuale

del materiale probatorio raccolto a seguito dell'intercettazione tra presenti operata con captatore informatico su dispositivo elettronico portatile. In particolare, al comma 1-*bis* dell'art. 270 c.p.p. si afferma che possono essere utilizzati i risultati delle intercettazioni tra presenti operate con trojan su dispositivo elettronico portatile anche per fornire la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione. Tale possibilità è ammessa qualora i risultati così acquisiti siano indispensabili per l'accertamento dei delitti indicati dall'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. e dei delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione, per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni.

Dall'analisi svolta si vuole evidenziare però come l'introduzione del d.lgs. 29 dicembre 2017, n. 216 abbia inteso regolare solo uno dei possibili usi dei captatori informatici, nello svolgimento delle attività investigative, attraverso l'inserimento del trojan all'interno di dispositivi elettronici portatili per effettuare intercettazioni tra presenti. Come visto infatti, il trojan ha una molteplicità di usi, tra cui la captazione dei dati in partenza e in arrivo su un dispositivo elettronico, l'acquisizione di comunicazioni e conversazioni avvenute mediante applicazioni di instant messaging, quali WhatsApp, Facebook messanger, Instagram, etc., l'attivazione del microfono o della telecamera, la possibilità di effettuare perquisizioni totali o parziali dell'hard disk, la possibilità di decifrare tutto ciò che viene digitato sul dispositivo bersaglio (la c.d. funzione *keylogger*[57]) e la possibilità di effettuare delle geolocalizzazioni.

Il captatore informatico è stato infatti definito un *congegno bulimico*[58] che da un remoto centro di comando carpisce tutte le informazioni necessarie acquisendole dal dispositivo bersaglio[59]. Nella prospettiva del cybercrime *de iure condendo* sarebbe auspicabile regolare gli usi – almeno quelli più comuni – del captatore informatico per eseguire le indagini, senza tralasciare la regolazione anche dell'inserimento del malware all'interno di dispositivi elettronici fissi, come per esempio le *smart tv*. In questo modo sarebbe possibile, da un lato avere una corretta qualificazione giuridica ogni qual volta il programma informatico venisse utilizzato mediante mezzi di ricerca della prova diversi dalle intercettazioni delle comunicazioni tra presenti, come, per esempio, le perquisizioni da remoto mediante virus trojan[60] e, dall'altro, la possibilità di ricercare una sempre maggiore tutela e un corretto bilanciamento tra il soddisfacimento dell'interesse pubblico nell'accertamento dei reati, previsto e tutelato dall'art. 112 Cost. relativo al principio dell'obbligatorietà dell'azione penale e, l'art. 15 Cost. che sancisce il principio di inviolabilità della riservatezza e segretezza di qualsiasi forma di comunicazione.

Dal punto di vista internazionale, a giudizio della Corte EDU, la compatibilità tra l'utilizzo dei captatori informatici nel corso dell'attività investigativa e la tutela del diritto alla riservatezza, di cui all'art. 8 CEDU, si basa sul rispetto di tre parametri fondamentali: la base giuridica appropriata, la finalità legittima e la necessità all'interno di una società democratica[61].

Nella sentenza *Zakharov c. Russia* del 2015, la Corte EDU precisa come non sia necessario indicare nel provvedimento autorizzativo delle intercettazioni i luoghi in cui le stesse debbano svolgersi, purché ne venga identificato il destinatario. Nell'utilizzo del trojan, il riferimento al luogo di svolgimento dell'intercettazione tra presenti non rappresenta il presupposto di autorizzabilità, necessario per il rispetto dell'art. 8 CEDU, secondo l'interpretazione data dalla giurisprudenza della Corte di Strasburgo. Difatti, è consentito, in via alternativa, far ricorso all'indicazione del destinatario dell'intercettazione tra presenti, anche in considerazione della natura dinamica e "itinerante" del mezzo utilizzato, che prescinde dal riferimento dei luoghi[62].

Dal punto di vista dell'ordinamento nazionale, affinché la Costituzione non sia violata è fondamentale constatare che vi sia il giusto bilanciamento tra il soddisfacimento dell'interesse pubblico nell'accertamento dei reati e il principio di inviolabilità della sfera di riservatezza e segretezza di qualsiasi forma di comunicazione[63].

La Corte costituzionale, nella sentenza n. 20 del 2017, ha evidenziato come i diritti di libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione sono oggetto del diritto inviolabile tutelato dall'art. 15 Cost., che garantisce «quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana» (citando le sentenze n. 366 del 1991 e n. 81 del 1993). Inoltre, i giudici delle leggi sottolineano che, al pari di ogni altro diritto costituzionalmente protetto, anche il diritto alla libertà e alla segretezza della corrispondenza può essere soggetto a limitazioni, purché disposte «per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge», poiché, se così non fosse, «si verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe "tiranno" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette» (sentenza n. 85 del 2013). Per questo, la «Costituzione italiana, come le altre Costituzioni democratiche e pluraliste contemporanee, richiede un continuo e vicendevole bilanciamento tra princìpi e diritti fondamentali, senza pretese di assolutezza per nessuno di essi», nel rispet-

to dei canoni di proporzionalità e di ragionevolezza (sentenza n. 85 del 2013). Pertanto, anche il diritto inviolabile protetto dall'art. 15 Cost. può subire limitazioni o restrizioni «in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante, sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse e sia rispettata la duplice garanzia» della riserva assoluta di legge e della riserva di giurisdizione (sentenza n. 366 del 1991)[64].

5. Conclusioni

Alla luce di quanto detto, si è voluto analizzare brevemente come, da un lato, la natura stessa del captatore informatico gli impedisca di essere adeguatamente regolato dal legislatore nazionale e, dall'altro, ci sia una continua osmosi tra gli ordinamenti giuridici internazionali per combattere il cybercrime. La natura dinamica, itinerante e le specifiche modalità attuative dei captatori informatici, utilizzati a fini investigativi per la persecuzione di gravi reati, comporta la necessità di una costante valutazione circa l'opportunità di tale peculiare mezzo di ricerca della prova e il rispetto del diritto alla riservatezza.

Nei prossimi anni l'Italia dovrà porsi, quali sempre più rilevanti obiettivi strategici, l'abbattimento del crimine informatico e un adeguato sviluppo di risorse tecnologiche per la sicurezza informatica in grado di creare sistemi "cyber resilienti".

Se, in un caso l'obiettivo è quello di tutelare le reti, i sistemi e servizi informativi, nell'altro si è voluto evidenziare come i malware, con la loro peculiare struttura, rappresentano degli importanti strumenti investigativi per garantire la sicurezza nazionale che necessitano di una più specifica regolazione, pur nei limiti della natura tecnologica e, inevitabilmente, "itinerante" del mezzo. Tali mezzi di utilizzo del captatore informatico rappresentano le due facce della stessa medaglia e di come questo possa cambiare la loro natura da "malevola in benevola".

Note

[1]La nozione è stata sviluppata da Vittorio Frosini. A lui si devono le prime riflessioni generali sul rapporto tra informatica, diritto e attività giudiziarie. Frosini è considerato il padre del c.d. umanesimo tecnologico. Egli affermò che ci si trovava dinnanzi a una nuova democrazia di massa in cui si realizza una nuova forma di libertà individuale e un potenziamento della forza intellettuale e operativa del singolo individuo all'interno della comunità.V. Frosini, *La democrazia nel XXI secolo*, Liberilibri, 2010.

[2]A tal riguardo, la Corte di Cassazione si pronunciò circa la contestazione al ricorrente di aver sottratto dei file al detentore e che tale spossessamento fosse avvenuto attraverso la copiatura di detti file. In merito, la Corte osservava come l'art. 624 c.p. avesse quale presupposto necessario l'impossessamento della cosa mobile altrui, sottraendola a chi la detiene. Nella fattispecie trattata, la copiatura dei file presupponeva che gli stessi fossero rimasti all'interno del computer, o del CD, del detentore e che il presunto agente nel reato di furto fosse entrato in possesso di una copia, senza che la precedente situazione di fatto fosse modificata a danno del soggetto già possessore dei file. Così facendo la Suprema Corte, sulla base dell'assenza del *fumus commissi delicti*, rilevando il difetto di motivazione disponeva l'annullamento con rinvio del provvedimento impugnato per un nuovo esame sul punto. Cass. Penale, Sez. IV, 13 novembre 2003, n. 3449. Successivamente, la Suprema Corte affermò il principio per cui, nel caso di riproduzione non autorizzata di programmi aziendali e di notizie riservate tramite l'accesso a un sistema operativo aziendale sussistono gli estremi per la configurazione del concorso tra accesso abusivo a un sistema informatico o telematico – art. 615-*ter* c.p. – e la frode informatica (art. 640-*ter* c.p.). Cass. Penale, Sez. II, 4 maggio 2006, n. 30663.

[3]C. Sarzana di S. Ippolito, *Informazioni, internet e diritto penale*, III ed., Giuffré, 2010, 288 p.

[4]Cass., Sez. un. 28 aprile 2016, n. 26889, Scurato, in CED Cass. n. 266905-266906.

[5]Quando l'inserimento avviene tramite posta elettronica il malware, allegato ad un messaggio, ha accesso più facile al sistema in quanto porta l'utente ad aprire il messaggio di posta con in allegato, ad esempio, un file di testo.

[6]Il supporto di memorizzazione – ad esempio, un'unità USB – serve a trasferire il malware nel sistema. Le modalità di trasporto e inserimento possono essere guidate tanto da colui che ha inserito il malware quanto dalla vittima, completamente inconsapevole. Questa modalità di inserimento del malware prevede, quindi, un accesso fisico al PC.

[7]Quando il malware viene inserito nel sistema informatico tramite il Web – in particolare, tramite un codice malevolo attraverso un download da una pagina Web – la vittima può svolgere sia un ruolo attivo sia passivo. Nel caso in cui svolga un ruolo attivo, l'utente contrae il malware scaricando un file, che appare "innocente" essendo in realtà malevolo. Nel secondo caso, invece, l'aggressore usa tecniche note come "drive-by download" che trasmettono un malware aprendo semplicemente una pagina Web. Con le misure di sicurezza assenti o compromesse, il malware attacca sulle vulnerabilità presenti nel browser evitando interazioni con l'utente-vittima.

[8]Talvolta, i malware assumono le sembianze di programmi essenziali per il funzionamento del sistema.

[9]Per quanto esistano diverse tecniche per la cifratura, quella più utilizzata sfrutta una chiave segreta secondo la crittografia simmetrica, ovvero l'utilizzo della stessa chiave sia per la crittazione che per la decrittazione.

[10]Il *kernel* è il nucleo di un sistema operativo. Il compito di questo software è quello di fornire un accesso sicuro all'hardware ai processi in esecuzione sull'elaboratore.

[11]M. Mezzalama, A. Lioy, H. Metwalley, *Anatomia del malware*, in "Mondo Digitale", n. 47, 2013.

[12]Google invece effettua controlli meno rigidi sugli sviluppatori e sulle applicazioni disponibili su Google Play; infatti, è possibile installare programmi esterni allo stesso.

[13]Il *drive-by download* si riferisce a due ambiti, entrambi riguardanti il download di un software da Internet: nel primo caso, ci si riferisce a quando l'utente accetta di scaricare un programma in modo automatico, nel secondo caso si fa riferimento al download che avviene senza che l'utente se ne accorga.

[14]Convenzione sulla criminalità informatica (STE n. 185), Budapest, 23 novembre 2001, entrata in vigore il 1º luglio 2004.

[15]L. Cuomo, R. Razzante, *La nuova disciplina dei reati informatici*, Giappichelli, 2009.

[16]Prima della Convenzione, ogni riferimento ai reati informatici riguardava, tanto nel Common law quanto nel Civil law, "la legge del mercato". Per tale si intende ambiti nei quali far rientrare il diritto d'autore e le leggi sui segreti industriali e commerciali.

[17]In Italia la Convenzione fu oggetto di ratifica con la legge 18 marzo 2008, n. 48. Nel Codice penale italiano vennero introdotti nuovi reati quali: il falso informatico, il danneggiamento informatico, la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, etc. Allo stesso modo, vennero effettuate delle modifiche al Codice di procedura penale nella sezione dei mezzi di ricerca della prova e in quella riguardante le indagini della polizia giudiziaria, con il fine di indicare specifiche modalità di compimento delle stesse attraverso regole volte all'indicazione di come effettuare le ispezioni, perquisizioni e sequestri, senza ledere i dati originali e con la massima conformità della copia all'originale.

[18]F. Resta, *Cybercrime e cooperazione internazionale, nell'ultima legge della legislatura*, in "Giurisprudenza di merito", 2008, n. 9, p. 2159.

[19]Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. La direttiva (UE) 2016/1148 è stata recepita nell'ordinamento nazionale attraverso il decreto legislativo 18 maggio 2018, n. 65, in vigore dal 24 giugno 2018. Il considerando (1) della direttiva afferma che «Le reti e i sistemi e servizi informativi svolgono un ruolo vitale nella società. è essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno». In tal senso, l'art. 1 della direttiva, nel delinearne l'oggetto e l'ambito di applicazione statuisce al par. 1 che «La presente direttiva stabilisce misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno».

[20]*Network and Information Security Directive.*

[21]R. Scavizzi, *Ue: nuove misure di contrasto agli incidenti informatici e alla criminalità telematica*, in "Eurocomunicazione", 29 luglio 2016.

[22]La direttiva NIS identifica i soggetti da tutelare dividendoli in due categorie: gli OES - *Operators of Essential Services* e i DSP - *Digital Service Providers*. Saranno poi gli Stati membri a definire quali delle proprie organizzazioni inserire. La direttiva è stata recepita nell'ordinamento nazionale attraverso il d.lgs. 18 maggio 2018, n. 65, anche detto decreto legislativo NIS, entrato in vigore dal 24 giugno 2018. Subito dopo l'adozione del decreto legislativo NIS, la normativa italiana sulla cybersecurity è stata rafforzata attraverso l'istituzione del perimetro di sicurezza nazionale cibernetica e i relativi decreti attuativi. La direttiva NIS sarà comunque oggetto di aggiornamento in quanto verrà sostituita dalla direttiva NIS 2 che amplierà i soggetti da tutelare includendo anche: le pubbliche amministrazioni, i service provider pubblici di comunicazione elettronica, i provider di servizi digitali, i fornitori del trattamento delle acque reflue e la gestione dei rifiuti, gli operatori nella fabbricazione di prodotti essenziali, i servizi postali e di corriere e il settore sanitario. Per un maggiore approfondimento si veda L. Sbriz, *Direttiva NIS, ecco i vantaggi per le aziende nell'usarla come linea guida sulla sicurezza*, in "CyberSecurity.it", 2022; M. Santarelli, *Verso la NIS 2, c'è l'accordo in Europa: ecco le novità su soggetti coinvolti e obiettivi*, *ivi*, 2022; L. Tosoni, *Direttiva NIS, così è l'attuazione italiana (dopo il recepimento): i punti principali del decreto*, in "AgendaDigitale.eu", 2021.

[23]Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»).

[24]*Ivi*, art. 2, 1).

[25]Per maggiori informazioni, si veda Consiglio europeo, *Cibersicurezza: la risposta dell'UE alle minacce informatiche*, novembre 2022.

[26]S.D. Warren, L.D. Brandeis, *The Right to Privacy*, in "Harvard Law Review", 1890, n. 4, p. 193 ss.

[27]Diritto al rispetto della vita privata e familiare. «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

[28]Art. 17 Patto internazionale relativo ai diritti civili e politici «1. Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. 2. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese».

[29]Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[30]Articolo 7 Carta dei diritti fondamentali dell'Unione Europea. *Rispetto della vita privata e della vita familiare* «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».

[31]Articolo 8 Carta dei diritti fondamentali dell'Unione Europea, *Protezione dei dati di carattere personale* «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[32]Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[33]M. Bassini, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in "Quaderni costituzionali", 2016, n. 3, p. 588.

[34]Sulla portata degli articoli 14 e 15 Cost. si veda P. Caretti, *I diritti fondamentali*, Giappichelli, 2011, p. 293. In particolare, si afferma che: «il diritto alla riservatezza viene definito come il diritto a mantenere riservato, salva espressa dichiarazione di volontà in senso contrario, quegli aspetti della propria vita privata, che attengono a fatti personalissimi che proprio per questo il soggetto ha il diritto di sottrarre alla conoscibilità dei terzi». Nel 1973 la Corte costituzionale in riferimento all'art. 15 Cost. ha affermato che «Questa norma non si limita a proclamare l'inviolabilità della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione (comma primo), ma enuncia anche espressamente che "la loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge" (comma secondo). Nel precetto costituzionale trovano perciò protezione due distinti interessi; quello inerente alla libertà ed alla segretezza

delle comunicazioni, riconosciuto come connaturale ai diritti della personalità definiti inviolabili dall'art. 2 Cost., e quello connesso all'esigenza di prevenire e reprimere i reati, vale a dire ad un bene anch'esso oggetto di protezione costituzionale». Corte Cost., 6 aprile 1973, n. 34, in "Consulta Online".

[35]A partire dalla sentenza del 27 maggio 1975, n. 2129, la Corte di Cassazione ha ritenuto definitivamente che l'ordinamento italiano riconoscesse il diritto alla riservatezza. La Corte affermava che il diritto in questione consisteva «nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze, che sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificate da interessi pubblici preminenti». Cass. Civ., Sez. I, 27 maggio 1975, n. 2129, in "Il Foro italiano", vol. 99, 1976, pp. 2895-2907. A titolo esemplificativo e non esaustivo si richiamano le successive pronunce della Corte di Cassazione che riconoscono quale *jus receptum* il diritto alla riservatezza: Cass., 5 aprile 1978, n.1557, in "Il Foro padano", I, 1979, p. 302; Cass. civ., Sez. III, 7 febbraio 1996, n. 982, in "Danno e responsabilità", 1996, p. 456; Cass., 7 febbraio 1996, n. 978, in "Corriere giuridico", 1996, n. 3, p. 264; Cass. Civ., Sez. III, 8 giugno 1998, n. 5658, in "Il Foro italiano", vol. 121, 1998, n. 9, pp. 2387-2394.

[36]L. 31 dicembre 1996 n. 675 (*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*); legge abrogata ai sensi dell'articolo 183, comma 1, lettera a), del Codice in materia di protezione dei dati personali.

[37]D.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali.*

[38]D.lgs. 10 agosto 2018, n. 101, *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).*

[39]In dottrina il tema è stato ampiamente trattato, *ex multis*: R. Flor, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di internet*, in "Diritto Penale Contemporaneo", 2012, pp. 1-13; F. Iovene, *Le cd. perquisizioni on line: tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in "Diritto Penale Contemporaneo", 2014, n. 3-4, pp. 329-342; E. Lorenzetto, *Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico"*, nota a Trib. Palermo, Sez. riesame, ord. 11 gennaio 2016, in "Diritto Penale Contemporaneo", 2016; L. Giordano, *Dopo le Sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, osservazioni a seguito di Cass., SSUU, sent. 28 aprile 2016, n. 26889, in "Diritto Penale Contemporaneo", 2017, n. 3, pp. 177-195.

[40]È importante sottolineare come i virus "spia" possano essere inseriti o all'interno di computer o all'interno di uno smartphone. Quando inseriti all'interno di uno smartphone assumono la veste o di un trojan come intercettatore ambientale – ovvero che capta comunicazioni tra presenti – o di un trojan come intercettatore telematico.

[41]Cass. Pen., Sez. VI, 8 aprile 2015, n. 27536; Cass. Pen., Sez. VI, 12 marzo 2015, n. 24237.

[42]Cass. Pen., Sez. VI, 26 maggio 2015, n. 27100, in CED Cass. n. 265654.

[43]P. Felicioni, *Le intercettazioni tra presenti mediante "captatore informatico" sono legittime nei procedimenti per delitti di criminalità organizzata*, in "Processo penale e giustizia", 2016, n. 5, pp. 118-138.

[44]Cass. Pen., Sez. VI, 10 marzo 2016, n. 13884.

[45]I quesiti sottoposti alle Sezioni Unite, con l'ordinanza n. 13884/16, cit. sono i seguenti: «se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi ove deve avvenire la relativa captazione; se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, cod. proc. pen.; se possa comunque prescindersi da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata».

[46]Cass., Sez. un. 28 aprile 2016, n. 26889, Scurato, cit. Sui temi di cui si occupa la sentenza si v. A. Camon, *Cavalli di Troia in Cassazione*, in "Archivio della nuova procedura penale", 2017, n. 1, pp. 91-100; A. Balsamo, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in "Cass. pen.", 2016, pp. 2274-2288; G. Corasaniti, *Le intercettazioni "ubiquitarie" e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*, in "Il Diritto dell'informazione e dell'informatica", 2016, p. 88; P. Felicioni, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in "Processo penale e giustizia", 2016, n. 5, p. 21; A. Gaito, S. Furfaro, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in "Archivio penale", 2016, n. 2, pp. 309-330; A. Cisterna, *Spazio ed intercettazioni, una* liaison *tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite*, *ivi*, pp. 331-347; L. Filippi, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)*, *ivi*, pp. 348-353; L. Picotti, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, *ivi*, pp. 354-365; L. Giordano, *Dopo le Sezioni unite sul "captatore informatico"*, cit.; G. Lasagni, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in "Diritto Penale Contemporaneo", 7 ottobre 2016, p. 22.

[47]La Corte di Cassazione ha affermato che erano inutilizzabili i risultati acquisiti con il trojan soltanto per i procedimenti aventi ad oggetto reati comuni, limitando l'impiego del captatore informatico ai reati di criminalità organizzata. Il luogo dell'intercettazione sarà indifferente, ai sensi dell'art. 13 d.l. 13 maggio 1991, n. 152, convertito con modificazioni dalla l. 12 luglio 1991, n. 203. L. Giordano, *La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità*, in "Diritto Penale Contemporaneo", 2017, n. 9, pp. 183-191.

[48]L. 23 giugno 2017, n. 103 *Modifiche al Codice penale, al codice di procedura penale e all'ordinamento penitenziario.* Entrata in vigore il 3 agosto 2017. Inoltre, l'art. 1, co. 84, lett. d), della legge n. 103 del 2017 ha delegato il Governo a adottare prescrizioni volte alla semplificazione «delle condizioni per l'impiego delle intercettazioni delle conversazioni e delle comunicazioni telefoniche e telematiche nei procedimenti per i più gravi reati dei pubblici ufficiali contro la pubblica amministrazione». Per un maggiore approfondimento, si veda L. Giordano, *La delega per la riforma della disciplina delle intercettazioni*, in A. Marandola, T. Bene (a cura di), "La riforma della giustizia penale", Giuffré, 2017, pp. 382 ss.

[49]D.lgs. 29 dicembre 2017, n. 216, *Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103.* L. Palmieri, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza*

"Scurato" alla riforma sulle intercettazioni, in "Diritto Penale Contemporaneo", 2018, n. 1, pp. 59-66. Il captatore informatico in materia di intercettazioni è oggetto della delega contenuta all'art. 1, co. 84, l. 23 giugno 2017, n. 103, c.d. *Riforma Orlando*. Nella Relazione illustrativa al d.lgs. 216/2017 si afferma che il delegante ha inteso regolare solo uno degli usi del captatore informatico, quale specifica modalità di intercettazione tra presenti, avente a oggetto solo i dispositivi mobili portatili. Difatti, a pagina 10 della Relazione illustrativa si evidenzia come il captatore informatico, consistendo in un malware, consente numerose operazioni, ma il delegante ha inteso limitare l'ambito applicativo dell'intervento normativo alla disciplina degli aspetti attinenti all'intercettazione audio, eseguita mediante inserimento del malware all'interno del dispositivo portatile, quali smartphone e tablet, e non anche di dispositivi fissi.

[50]Si veda G. Di Paolo, *Le intercettazioni mediante l'uso di captatore informatico*, in A. Giarda, F. Giunta, G. Varraso (a cura di), "Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura", Cedam-Wolters Kluwer, 2018, pp. 165 ss.; L. Giordano, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in "Sistema Penale", 2020, n. 4, pp. 109-143.

[51]Il comma 2, dell'art. 266 c.p.p. è stato modificato dall'art. 4, d.lgs. 216/2017 con decorrenza dal 26 gennaio 2018. Inoltre, quanto previsto dal comma 2, dell'art. 266 c.p.p. trovava applicazione alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 marzo 2019. Successivamente, il d.lgs. 216/2017, come modificato dalla l. 30 dicembre 2018, n. 145, ha disposto, con l'art. 9, comma 1, che le disposizioni degli artt. 2, 3 4, 5 e 7 si applicassero alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 luglio 2019.

[52]Inoltre, il comma 2-*bis* dell'art. 266 c.p.p. afferma che l'intercettazione di comunicazioni tra presenti mediante l'uso del trojan inserito su dispositivo elettronico portatile è consentita, previa indicazione delle ragioni che ne giustificano l'uso anche nei luoghi di privata dimora, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione.

[53]Il comma 1 è stato modificato dall'art. 2, co. 1, lett. d) del d.l. 30 dicembre 2019, n. 161, convertito con modificazioni dalla l. 28 febbraio 2020, n. 7. Il d.l. 161/2019, convertito con modificazioni dalla l. 28 febbraio 2020, n. 7, ha disposto, con l'art. 2, co. 8, che «Le disposizioni del presente articolo si applicano ai procedimenti penali iscritti successivamente al 30 aprile 2020».

[54]Cfr. p. 10 della Relazione illustrativa al d.lgs. 216/2017.

[55]Il comma 2-*bis* dell'art. 267 c.p.p. è stato inserito dall'art. 4, d.lgs. 216/2017 con decorrenza dal 26 gennaio 2018 e applicazione alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 marzo 2019. In un secondo momento, il d.lgs. 216/2017, come modificato dalla l. 30 dicembre 2018, n. 145, con l'art. 9, co. 1 ha disposto che «Le disposizioni di cui agli articoli 2, 3 4, 5 e 7 si applicano alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 luglio 2019». Tale comma è stato poi modificato dall'art. 2, co. 1, lett. d) del d.l. 161/2019, convertito con modificazioni dalla l. 28 febbraio 2020, n. 7. Il d.l. 161/2019 ha poi disposto che le disposizioni dell'art. 2 si applicano ai procedimenti penali iscritti successivamente al 30 aprile 2020».

[56]La Suprema Corte ha precisato che «È tuttavia necessario, come stabilito nella citata pronuncia delle Sezioni Unite, il rispetto di un onere motivazionale rafforzato ai fini della emissione del provvedimento autorizzativo, poiché la forza intrusiva del mezzo usato ed il potenziale *vulnus* all'esercizio delle libertà costituzionalmente tutelate devono essere prudentemente bilanciati con il rispetto dei canoni di proporzione e ragionevolezza, cosicché la qualificazione, pure provvisoria, del fatto come inquadrabile in un contesto di criminalità organizzata risulti ancorata a sufficienti, sicuri ed obiettivi elementi indiziari che ne sorreggano, per un verso, la corretta formulazione da parte del Pubblico Ministero e, per altro verso, ne consentano la successiva, rigorosa, verifica dei presupposti da parte del Giudice chiamato ad autorizzare l'esecuzione delle relative operazioni di intercettazione». Cass., Sez. VI, sent. 13 giugno 2017, n. 36874. Per un maggiore approfondimento, la sentenza è stata commentata da L. Giordano, *La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità*, in "Diritto Penale Contemporaneo", 2017, n. 9, pp. 183-191.

[57]In questo caso si è espressa la giurisprudenza di legittimità e, nel caso di specie, il virus trojan era stato utilizzato per acquisire delle password di accesso agli account di posta elettronica degli imputati. Ottenute queste password, gli inquirenti avevano potuto prendere visione sia dei messaggi che venivano inviati o ricevuti nella casella di posta elettronica che dei messaggi che venivano salvati nella cartella denominata bozze. La Suprema Corte ha ritenuto legittimo l'uso di un programma informatico per acquisire le credenziali di accesso alla casella di posta elettronica. Si veda Cass., Sez. IV, 28 giugno 2016, n. 40903, in CED Cass. n. 268228.

[58]L'espressione è stata coniata da L. Filippi, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, in "ilpenalista.it", 2016.

[59]L. Palmieri, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali*, cit., p. 60.

[60]Nel caso delle perquisizioni da remoto mediante virus trojan, la Corte costituzionale tedesca ha sottolineato quali siano i limiti giuridici dell'attività investigativa compiuta con mezzi di ricerca della prova che acquisiscano informazioni da remoto. Si veda *Bundersverfassungsgericht*, 27 febbraio 2008, in "Rivista trimestrale di diritto penale dell'economia", 2009, n. 3, p. 679. La Corte costituzionale tedesca, con la pronuncia appena citata ha dichiarato l'incostituzionalità delle disposizioni di legge che permettevano alla polizia federale, nei limiti del delitto di terrorismo internazionale, di ricorrere a misure di sorveglianza definite come occulte, tra cui la perquisizione da remoto. Sul punto si veda A. Balsamo, *Intercettazioni ambientali mobili e cooperazione giudiziaria internazionale: le indicazioni desumibili dalla giurisprudenza della Corte di Strasburgo*, in "Cassazione penale", 2016, n. 11, p. 4236. Per quanto riguarda la giurisprudenza nazionale si veda Cass., Sez. V, 14 ottobre 2009, n. 16556, in CED Cass. n. 246954 che è stata così massimata «È legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel "personal computer" in uso all'imputato e installato presso un ufficio pubblico, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati. (Nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'"hard disk" del computer in uso all'imputato, aveva avuto ad oggetto non un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elettronico", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen.)».

[61]Corte EDU, Grande Camera, *Zakharov c. Russia*, ricorso n. 47143/06, 4 dicembre 2015, par. 227 ss.

[62]Cass., Sez. V, 30 settembre 2020, n. 35010.

[63]Nella sentenza 35010 del 2020 la Corte di Cassazione afferma che «sono, dunque, i mezzi di ricerca della prova a dover

essere coperti da riserva di legge, ma non le specifiche modalità attuative, influenzate da materiali questioni pratiche o di sviluppo tecnologico, a godere della medesima riserva, rimanendo evidente, peraltro, che l'unico profilo oggetto di verifica di costituzionalità sia quello relativo al fatto che "il legislatore abbia operato in concreto un bilanciamento tra il principio costituzionale della tutela della riservatezza nelle comunicazioni e l'interesse della collettività, anch'esso costituzionalmente protetto, alla repressione degli illeciti penali, senza imporre limitazioni irragionevoli o sproporzionate dell'uno o dell'altro (sentenza n. 372 del 2006)"». Cass., Sez. V, 30 settembre 2020 n. 35010.

[64]Cfr. punto 3.1. della sentenza della Corte costituzionale, n. 20 del 2017.

* * *

Profiles of the fight against cybercrime *in iure condito* and *de iure condendo*

Abstract: In the digital era, our lives are now inextricably linked to smartphones and tablets that follow us on our every move. It is precisely the itinerant nature of these media that makes them perfect 'containers' for hosting so-called cyber-captors, i.e., malware used for investigative purposes, for the prosecution of crimes. Thus, we examine how the case-law and the legislature have tried to rule on the advent of these new means of searching for evidence in an attempt to find a balance between satisfying the public interest in the investigation of crimes, provided for and protected by Article 112 of the Constitution on the principle of mandatory prosecution and Article 15 of the Constitution, which enshrines the principle of inviolability of confidentiality and secrecy of any form of communication. At the same time, however, it should be emphasized that the fight against cybercrime is essential, which is also implemented using such tools and an adequate development of technological resources for cyber security capable of creating systems that are 'cyber resilient'. In this sense, the dual nature, benevolent and malevolent, of the same means, malware, is brought to light.

Keywords: Malware – Cybersecurity – Cybercrime – Right to privacy – Cyber capturing