ISSN 1125-856X

Cassazione penale

direttore scientificoc **Domenico Carcano**
ondirettore **Mario D'Andria**
LIX - Novembre 2019, n°**11**

II 2019

| estratto

SPY-SOFTWARE: GLI OSCILLANTI CONFINI DELLA LEGALITÀ

con nota di Myriam Caroleo Grimaldi

GIUFFRÈ FRANCIS LEFEBVRE

467.5 GLI *SPY-SOFTWARE* VANNO INCLUSI TRA GLI APPARATI E GLI STRUMENTI DI CUI ALL'ART. 617-*BIS*, COMMA 1, C.P.

Sez. V - Ud. 18 marzo 2019 (dep. 5 aprile 2019), n. 15071 - Pres. Sabeone - Rel. Scordamaglia - P.M. Marinelli (concl. conf.) - (275104)

INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE OD IMPEDIRE COMUNICAZIONI O CONVERSAZIONI TELEGRAFICHE O TELEFONICHE - "*Spy-software*" - Inclusione tra gli apparati e strumenti di cui all'art. 617-*bis*, comma 1, c.p. - Sussistenza - Fondamento.
(C.p. art. 617-*bis*)

*I programmi informatici denominati "*spy-software*" che, se installati in modo occulto su un telefono cellulare, un "*tablet*" o un PC, consentono di captare tutto il traffico dei dati in arrivo o in partenza dal dispositivo, rientrano tra gli "apparati, strumenti, parti di apparati o di strumenti" diretti all'intercettazione o all'impedimento di comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone, di cui all'art. 617-*bis*, comma 1, c.p., in quanto tale norma delinea una categoria aperta, suscettibile di essere implementata per effetto delle innovazioni tecnologiche che, nel tempo, consentono di realizzare gli scopi vietati dalla legge.*

RITENUTO IN FATTO - 1. V.A., per il tramite del difensore, ricorre avverso la sentenza della Corte di appello di Milano del 21 febbraio 2018, che ha confermato la sentenza del Tribunale di Busto Arsizio del 3 aprile 2017, emessa nei suoi confronti, in punto di declaratoria di responsabilità per il delitto di cui all'art. 617-*bis* c.p., commesso in pregiudizio della coniuge M.L., con l'istallare all'interno del telefono cellulare a lei in uso uno *spy-software* idoneo ad intercettarne le comunicazioni telefoniche.

2. L'atto di impugnativa è affidato a due motivi – enunciati nei limiti necessari per la motivazione ai sensi dell'art. 173 disp. att. c.p.p. –, che denunciano:

2.1. il vizio di violazione di legge, in relazione all'art. 617-*bis* c.p., e art. 14 preleggi, e il vizio di motivazione, sul rilievo dell'applicazione analogica della norma incriminatrice in ragione dell'assimilazione all'"apparato o allo strumento" da essa contemplato del programma informatico installato all'interno del telefono cellulare della persona offesa;

2.2. il vizio di violazione di legge, in relazione agli artt. 49, 50 e 617-*bis* c.p., e il vizio di motivazione, essendo il fatto di reato scriminato dal consenso dell'avente diritto, posto che la destinataria delle intrusioni era stata informata dal figlio dell'istallazione del software sul proprio cellulare, e, perciò, non aveva, in concreto, subito alcuna lesione della propria libertà di comunicazione.

CONSIDERATO IN DIRITTO - Il ricorso è infondato.

1. Le Sezioni unite di questa Corte, con la sentenza n. 26889 del 28/4/2016, Scurato, Rv. 266905, hanno spiegato che l'evoluzione tecnologica ha consentito di approntare strumenti informatici del tipo "*software*", solitamente istallati in modo occulto su un telefono cellulare, un *tablet* o un PC, che consentono di captare tutto il traffico dei dati in arrivo o in partenza dal dispositivo e, quindi, anche le conversazioni telefoniche.

Ne viene che, al lume di tale autorevole interpretazione del diritto vivente, non è possibile dubitare dell'inclusione dei programmi informatici denominati "*spy-software*" nella categoria degli "apparati, strumenti, parti di apparati o di strumenti" diretti all'intercettazione o all'impedimento di comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone, di cui all'art. 617-*bis* c.p., comma 1, venendo in rilievo una categoria aperta e dinamica, suscettibile di essere implementata per effetto delle innovazioni

tecnologiche che, nel tempo, consentono di realizzare gli scopi vietati dalla legge. Da ciò deriva l'infondatezza del primo motivo.

2. Parimenti infondato è il secondo motivo. Appartiene al patrimonio condiviso di questa Corte l'enunciazione direttiva secondo la quale il reato previsto dall'art. 617-*bis* c.p., anticipa la tutela della riservatezza e della libertà delle comunicazioni mediante l'incriminazione di fatti prodromici all'effettiva lesione del bene, punendo l'installazione di apparati o di strumenti, ovvero di semplici parti di essi, per intercettare o impedire comunicazioni o conversazioni telefoniche; pertanto, ai fini della configurabilità del reato deve aversi riguardo alla sola attività di installazione e non a quella successiva dell'intercettazione o impedimento delle altrui comunicazioni, che rileva solo come fine della condotta, con la conseguenza che il reato si consuma anche se gli apparecchi installati, fuori dall'ipotesi di una loro inidoneità assoluta, non abbiano funzionato o non siano stati attivati (Sez. II, n. 37710 del 24/9/2008, Pariota, Rv. 241456; nello stesso senso: Sez. V, n. 37557 del 12/5/2015, Sinisi, Rv. 265789; Sez. V, n. 3061 del 14/12/2010 - dep. 27/1/2011, Mazza, Rv. 249508). Ne viene che le deduzioni difensive in ordine all'eventuale esistenza del consenso all'intrusione, desumibile dal comportamento inerte della detentrice del telefono cellulare interessato dal software, ed in ordine all'assenza di un'effettiva lesione della libertà delle comunicazioni della destinataria delle condotte intrusive sono prive di rilievo, perché si riferiscono ad una situazione – la captazione delle comunicazioni telefoniche – che rappresenta un *post-factum* rispetto al momento di consumazione del reato, coincidente con l'installazione del *software*.

3. S'impone, dunque, il rigetto del ricorso con conseguente condanna del ricorrente al pagamento delle spese processuali, nonché alla rifusione delle spese in favore della sola M.L., che liquida in complessivi euro 2.500,00 oltre accessori di legge.

4. Con riguardo al profilo delle statuizioni civili, è d'uopo precisare che nulla è dovuto a Ve. Am., che pure ha fatto richiesta di liquidazione delle spese del presente grado di giudizio, non figurandovi come parte resistente: egli, infatti, ha assunto la veste di parte offesa, costituita parte civile, in relazione al solo delitto di cui all'art. 617-*quinquies* c.p., (capo 2 della contestazione), rispetto al quale, tuttavia, la Corte territoriale, all'esito del giudizio di appello, ha dichiarato non doversi procedere nei confronti dell'imputato per essere il reato estinto per intervenuta prescrizione.

SPY SOFTWARE: GLI OSCILLANTI CONFINI DELLA LEGALITÀ

Spy Software: the Oscillants Borders of Legality

La quinta sezione della suprema Corte, con la sentenza n. 15071 - RV. n. 275104, ha ritenuto indubbia l'appartenenza dei programmi "*spy-software*" alla categoria degli "strumenti o parti di strumenti" contemplati dall'art. 617-*bis* c.p. La sentenza in commento pare di estrema attualità, in quanto offre spunti di riflessione che, partendo dall'enunciato esposto dall'art. 617-*bis* c.p., passando in rassegna le numerose riforme normative intervenute per far fronte all'inarrestabile evoluzione tecnologica, approdano a un nuovo concetto di "riservatezza", con cui il Legislatore si dovrà confrontare.

The fifth section of the Supreme Court, with sentence n. 15071 – RV. 275104 has deemed undoubtedly the belonging of the "spy-software" programs to the category of "instruments or parts of instruments" contemplated by art. 617-bis Criminal Code. The sentence in question seems to be extremely topical, as it offers insights that, starting from the statement exposed by the law in question, reviewing the numerous reforms made to face the relentless technological evolution, arrive at a new concept of "privacy", with which the Legislator will have to confront.

(Traduzione in inglese a cura dell'Autrice)

di **Myriam Caroleo Grimaldi**
Avvocato

Sommario **1.** Profili giuridici e approdi giurisprudenziali sul reato di installazione di apparecchiature atte a intercettare. — **2.** Riservatezza e esigenze investigative dagli albori del primo intervento del legislatore, alla riforma del 1993. Cenni storici. — **3.** La sentenza Scurato e nuovi approdi raggiunti in tema di intercettazioni: l'agente intrusore informatico. — **4.** Intercettazioni e *trojan*: il d.lg. 29 dicembre 2017, n. 216 e legge n. 3/2019. — **5.** Il fenomeno degli *spy-software* e le tutele per la commercializzazione, tra cautele per chi acquista, violazioni della *pricacy* e *social network*. — **6.** Conclusione.

1. PROFILI GIURIDICI E APPRODI GIURISPRUDENZIALI SUL REATO DI INSTALLAZIONE DI APPARECCHIATURE ATTE A INTERCETTARE

Il Legislatore dell'epoca, nell'introdurre nel nostro ordinamento il precetto penale codificato nell'art. 617-*bis* c.p., molto opportunamente lo aveva rubricato nel novero dei delitti contro l'inviolabilità dei segreti, con riferimento al paradigma di cui agli artt. 14 e 15 Cost., utilizzando concetti aperti all'evoluzione tecnologica «... apparati, strumenti, parti di apparati o di strumenti ...» sebbene che all'epoca della l. n. 98/1974 non potesse certo immaginare un'evoluzione capace di concepire una tecnologia idonea a consentire una sofisticata ed invasiva lesione della sfera privata, anche a distanza.

Indagando i tratti essenziali, si rileva trattarsi di un reato di pericolo che anticipa la soglia di punibilità propria dell'art. 617 c.p., di talché, la violazione della norma richiede semplicemente l'installazione di elementi idonei ad intercettare/impedire le conversazione, non richiedendo quindi né che l'intercettazione della comunicazione o la sua interruzione sia effettivamente avvenuta; né che il soggetto nei confronti del quale sia stata perpetrata la condotta intrusiva ne avesse consapevolezza, nei termini di un eventuale consenso dell'avente diritto.

Queste circostanze, infatti, rappresentano il fine della condotta, ossia un mero *post factum*, rispetto all'attività di installazione degli "strumenti o parti di strumenti" atti a intercettare, richiamati dalla lettera dell'art. 617-*bis*c.p,

Ne discende, sotto il profilo della consumazione del delitto, che l'attività di installazione sia da sola sufficiente a determinarne l'integrazione, esclusa solo nel caso di una accertata assoluta inidoneità del congegno adoperato [1].

In questo quadro si inserisce la pronuncia in commento, con cui la quinta sezione della suprema Corte, sentenza emessa il 5 aprile 2018, n. 15071 – in *C.E.D. Cass*., n. 275104 –, si è occupata di ribadire un principio di diritto del tutto consolidato, ritenendo integrata la fattispecie p. e p. dall'art. 617-*bis* c.p. nel caso del marito che installi nel dispositivo cellulare in uso a sua moglie strumenti capaci di intercettarne le conversazioni.

Il ragionamento della suprema Corte ha preso le mosse dalla consolidata esegesi del concetto di intercettazione, che si riferisce alla presa di cognizione di conversazioni che intercorrono fra soggetti diversi da chi registri o prenda effettiva cognizione del contenuto delle conversazioni medesime, la sentenza emessa ha, dunque, riaffermato il principio, secondo cui il delitto di cui all'art. 617-*bis* c.p. è posto a presidio della tutela del diritto alla riservatezza e della libertà delle comunicazioni, mediante l'incriminazione di condotte prodromiche alla

———

[1] Sez. II, 3 ottobre 2008, n. 37710/2008, in *C.E.D. Cass*., n. 241456.

lesione del bene, letteralmente punendo l'attività di istallazione di strumenti o apparati finalizzati a intercettare o impedire le comunicazioni telefoniche [2].

La Cassazione ha poi osservato che, se è vero che il Legislatore ha inteso sanzionare la semplice installazione di apparecchiature del tipo sopra descritto, o anche solo di parti di esse, è altrettanto indiscutibile che il dettato normativo sia chiaro nel prevedere che la condotta, per rivestire valenza penale, debba essere finalizzata a «intercettare o impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone». Dunque, a fare in modo che l'agente, attraverso l'indebita captazione del flusso di notizie fra soggetti terzi, consentita dalle apparecchiature medesime, possa acquisire dati scambiatisi dagli interlocutori, ovvero precludere loro detto scambio.

Dunque, ha infine concluso la Corte, alla luce delle innovazioni tecnologiche che consentono di captare l'intero traffico telefonico, è fuor di dubbio che debbano includersi nell'alveo degli "strumenti o apparati" diretti all'intercettazione, i programmi "*spy-software*", rigettando il ricorso sulla base delle considerazioni di cui si è scritto e sulla scia di precedenti giurisprudenziali riguardanti casi analoghi.

Si tratta, infatti, solo di verificare se tra le potenzialità dei programmi istallati vi sia la realizzazione dello scopo vietato; programmi il cui censimento, alla luce della rapidità degli sviluppi in campo tecnologico costantemente e progressivamente raggiunti o raggiungibili, appare impossibile.

Non a caso, la sentenza emessa dalla V sezione, ampliando il novero delle captazioni penalmente sanzionabili, ha superato la prima delle doglienze rappresentate in sede di ricorso, muovendo dalla constatazione che, alla luce della sentenza "Scurato", la dicitura "apparati o strumenti" debba intendersi come "categoria aperta e dinamica", a cui non sfuggono i programmi di nuova generazione [3].

L'art. 617-*bis* c.p. era nato, d'altronde, proprio dal rilievo che la tecnologia aveva reso disponibili mezzi particolarmente insidiosi, capaci di captare dati sensibili, in maniera sempre più penetrante.

La pronuncia in esame, dunque, trova soluzione mediante l'autorevole richiamo alla recente giurisprudenza delle Sezioni unite, che si era espressa sulla legittimità dell'utilizzo ai fini investigativi del cd "agente intrusore", argomento su cui dottrina e giurisprudenza hanno a lungo dibattuto [4].

La citata sentenza Scurato fornisce la seguente definizione del *software trojan horse*:

Il programma informatico viene installato in un dispositivo del tipo *target* (un computer, un *tablet* o uno *smartphone*), di norma a distanza e in modo occulto, per mezzo del suo invio con una mail, un sms o un'applicazione di aggiornamento. Il *software* è costituito da due moduli principali: il primo (server) è un programma di piccole dimensioni che infetta il dispositivo bersaglio; il secondo (client) è l'applicativo che il virus usa per controllare detto dispositivo.

———

[2] Sez. V, 27 gennaio 2011, n. 3061, in *C.E.D. Cass.*, n. 249508; Sez. V, 30 agosto 2018, *ivi*, n. 273768; Sez. V, 16 settembre 2015, n. 37557, *ivi*, n. 265789; Sez. V, 3 ottobre 2008, n. 37710, *ivi*, n. 241456; Sez. V, 18 marzo 2003, n. 12698, *ivi*, n. 731

[3] Sez. un., 1° luglio 2016, n. 26889, in *C.E.D. Cass.*, n. 266905.

[4] Cfr. Orlandi, *Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Archivio pen.* (web), 25 luglio 2016; Giordano, *dopo le sezioni unite sul captatore informatico Avanzano le nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. pen. cont.*, 3/2017, p. 177

Uno strumento tecnologico di questo tipo consente lo svolgimento di varie attività e precisamente:

– di captare tutto il traffico dati in arrivo o in partenza dal dispositivo "infettato" (navigazione e posta elettronica, sia web mali, che *out look*);

– di attivare il microfono e, dunque, di apprendere per tale via i colloqui che si svolgono nello spazio che circonda il soggetto che ha la disponibilità materiale del dispositivo, ovunque egli si trovi;

– di mettere in funzione la web camera, permettendo di carpire le immagini;

– di perquisire lo *hard disk* e di fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira;

– di decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (*keylogger*) e visualizzare ciò che appare sullo schermo del dispositivo bersaglio (*screenshot*);

– di sfuggire agli antivirus in commercio.

I dati raccolti sono trasmessi, per mezzo della rete internet, in tempo reale o ad intervalli prestabiliti ad altro sistema informatico in uso agli investigatori.

L'avvento dei programmi informatici di nuova generazione, presi in esame dalla legislazione in tema di *cybercrimes*, ha reso la norma in argomento di grande attualità: videofonini, *tablet* e personal computer fanno, oramai, parte del vivere quotidiano e costituiscono al contempo strumento di possibili aggressioni, peraltro alla portata di tutti. Ne è testimonianza il fiorire di giurisprudenza che vi si confronta quotidianamente, nel tentativo di potenziare il regime delle prove nell'ambito investigativo, dilatando, contestualmente, le maglie della norma penale.

Sono quindi le attuali e crescenti innovazioni informatiche, il tema portante della sentenza in commento.

2. RISERVATEZZA E ESIGENZE INVESTIGATIVE DAGLI ALBORI DEL PRIMO INTERVENTO DEL LEGISLATORE, ALLA RIFORMA DEL 1993. CENNI STORICI

Nel commentare l'esito raggiunto dalla quinta sezione della Cass. sent., il 5 aprile 2018, n. 15071 – in *C.E.D. Cass*., n. 275104 –, non si può prescindere da un cenno sull'elaborazione normativa che si è sviluppata in tema di intercettazioni, dalla prima riforma operata dal Legislatore nel 1974, all'ultima, attualmente ancora in attesa di essere promulgata.

Con la l. 8 aprile 1974, n. 98 sulla Tutela della riservatezza e della libertà e segretezza delle comunicazioni, per la prima volta, il Legislatore interveniva a contrastare le nuove minacce tecnologiche, capaci di invadere la sfera privata, al di là di quanto allora fosse da ritenersi neppure verosimile.

Le numerose discussioni parlamentari che precedettero l'entrata in vigore della legge, proposta al fine di adeguare al mutato contesto sociale la disciplina delle intercettazioni legali, portarono all'inserimento di nuove fattispecie, tra le quali l'art. 615-*bis* c.p. – Interferenze illecite nella vita privata, inserito all'art. 1 della legge; alla sostituzione dell'art. 617 c.p. – Cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche –, inserito all'art. 2; alla formulazione degli artt. 617-*bis* - Istallazione di apparecchiature atte a intercettare o impedire comunicazioni o conversazioni telegrafiche o telefoniche – e *ter* – Falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche – inseriti all'art. 3; e a quella dell'art. 623-*bis* c.p. – Comunicazioni e

conversazioni non telegrafiche o telefoniche, inserito all'art. 4, che estendeva le disposizioni contenute nella sezione relativa alle comunicazioni e conversazioni telegrafiche o telefoniche, "a qualunque altra trasmissione di suoni, immagini o altri dati effettuata con collegamento su filo o ad onde guidate".

Gli articoli successivi – artt. 5, 6 e 7 – intervenivano a modificare il codice di procura penale, aggiungendo gli artt. 226-*bis*, *ter*, *quater* e *quinquies* c.p.p. – art. 5 –; sostituivano l'art. 339 c.p.p. – art. 6 –; e aggiungevano un capoverso all'art. 423 c.p.p. – art. 7 –.

Le disposizioni transitorie e finali erano affidate ai residui artt. 8, 9, 10 e 11.

In particolare, l'art. 9 incaricava il Ministro per le poste e le telecomunicazioni, di concerto con il Ministro per l'interno e con quello per l'industria, il commercio e l'artigianato, a provvedere con propri decreti all'elencazione degli «apparecchi o strumenti e delle parti di apparecchi o strumenti», idonei in modo non equivoco a operare le riprese di immagini o le intercettazioni di comunicazioni o conversazioni, di cui agli artt. 615-*bis* e 617 c.p.

Si disponeva altresì che «chiunque, senza licenza del Ministro per le poste e le telecomunicazioni, da concedersi sentito il parere del Ministro per l'interno, fabbrica, importa, acquista, vende, trasporta, noleggia o in qualsiasi altro modo mette in circolazione gli apparecchi o strumenti indicati nei precedenti commi, o parti di essi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni e con la multa da lire un milione a lire cinque milioni».

La tecnologia, considerata nei limiti di una plausibilità superabile solo dall'immaginazione, già in quegli anni era avvertita, da un lato, come un potenziale rischio per la libertà della persona; dall'altro, come uno stimolo per nuove sfide in capo giuridico [5].

Successivamente, agli inizi degli anni 90, il Legislatore interveniva nuovamente con la legge n. 547/1993, che modificava e integrava norme del codice penale e del codice di procedura penale in tema di criminalità informatica, estendendo il novero degli articoli sopra menzionati o comunque aggiungendo a fattispecie già previste, ipotesi che puntualmente contemplavano la tecnologia informatica e i suoi contenuti, tal volta come oggetto di tutela, talaltra come strumento da cui difendersi.

Così venivano apportate modifiche agli artt. 392, 420 c.p.; veniva aggiunto l'art. 490-*bis* c.p.; gli artt. 615-*ter*, *quater*, *quinquies* c.p.; l'art. 617-*sexies* c.p. e modificato l'art. 621 c.p.

Attraverso l'art. 623-*bis* c.p. [6] si è provveduto a estendere ulteriormente la circonferenza normativa anche alle comunicazioni effettuate mediante onde elettriche, inserendole nel novero delle trasmissioni a distanza di suoni immagini e altri dati tutelati a norma dell'art. 617-*bis* c.p.

Si aggiungevano le ipotesi di frode informatica – art. 640-*ter* c.p. – e di danneggiamento di sistemi informatici – art. 635-*bis* c.p. –.

———

[5] Cfr. Minotti, in *Guida dir.*, 3 gennaio 2009, n. 1 p. 93 che ha approfondito il tema dell'inviolabilità del domicilio informatico, alla luce della sentenza emessa dalla Sez. V, 26 novembre 2008, n. 44156; sul punto cfr. sentenza 27 febbraio 2008, in *Riv. trim. dir. pen. econ.*, 3, 2009, p 679 ss., con nota Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsggericht sulla cd. On line durchuchung*, sentenza che ha riconosciuto l'inadeguatezza dei diritti a tutela delle libertà di domicilio e delle comunicazioni a dare copertura sufficiente allo spazio digitale, inaugurando il diritto alla cd. "autodeterminazione informativa" e "sicurezza informatica" di rango costituzionale

[6] L'art. 8 della l. n. 547/1993 ha modificato l'art. 623-*bis*, sostituito dal seguente: «Art. 623-*bis*. - (Altre comunicazioni e conversazioni).- Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza dei suoni, immagini o altri dati».

Si provvedeva, altresì, a un ulteriore adeguamento della disciplina delle intercettazioni – art. 268 c.p.p. –, aprendo all'impiego di impianti privati per le operazioni di captazione e ai flussi relativi ai sistemi informatici.

Con uno sguardo attento ai temi "tutela e tecnologia" – segnatamente di alcune fattispecie introdotte dalla legge n. 547/1993 – deve concludersi che la tecnologia è ritenuta oggetto di tutela, a esempio, con il riconoscimento giuridico del cosiddetto domicilio informatico, una nuova e tecnologica forma di domicilio, sempre riconducibile alla già citata copertura costituzionale.

L'esegesi normativa sviluppatasi recentemente sul punto, rileva con chiarezza la diretta discendenza della violazione di domicilio e la perfetta collocazione nell'alveo dei diritti presidiati dall'articolo 14 della Costituzione, fissando un inscindibile vincolo tra riservatezza e domicilio.

All'epoca della riforma del 1974, infatti, la tecnologia era concepita come strumento di possibili abusi verso i medesimi ambiti protetti dagli artt. 14 e 15 Cost., prolungando le ingerenze agli atti di intrusione non fisica, ma a distanza, mediante l'uso di strumenti di captazione.

In altri termini, nonostante da quegli anni ci separi una distanza siderale, già cominciava, seppur lentamente, l'ascesa di una tecnologia avanzata, capace di fornire mezzi di ricerca della prova sofisticati e penetranti, fondamentali nella lotta alla criminalità organizzata; ma contestualmente lesivi di diritti costituzionalmente protetti e avvertiti di tale portata, da ritenere altrettanto necessario inserire fattispecie che sapessero fronteggiarne l'utilizzo *contra legem*, censirne le potenzialità dannose per arginarle ovvero ampliare i confini di esistenti delitti, al fine di tutelarla.

3. LA SENTENZA SCURATO E NUOVI APPRODI RAGGIUNTI IN TEMA DI INTERCETTAZIONI: L'AGENTE INTRUSORE INFORMATICO

Nel caso della sentenza Scurato, l'impiego dello strumento per la realizzazione delle intercettazioni "tra presenti" è stato ritenuto legittimo in applicazione dall'art. 13 d.l. n. 151/1991, convertito dalla legge n. 203/1991, che consente la captazione anche nei luoghi di privata dimora, in deroga ai presupposti stabiliti dall'art. 266, comma 2, c.p.p., nei soli procedimenti per i delitti di criminalità organizzata.

I profili giuridici che si andavano delineando inerivano, in primo luogo, la tenuta costituzionale dei captatori informatici, installati nei dispositivi elettronici portabili (cellulari, *tablet* e *computer*), nei termini di una riconosciuta necessità di bilanciamento, tra esigenze investigative e diritti individuali, riconoscendo la formidabile invadenza dei programmi inoculati.

In secondo luogo, la questione riguardava l'impossibilità di sospenderne l'azione o di predeterminarne né prevedere il luogo in cui il dispositivo venisse introdotto, con la conseguenza che il mezzo adoperato, divenuto incontrollabile, finisse per superare i limiti imposti dall'art. 266, comma 2, c.p.p., intercettando comunicazioni tra presenti all'interno del domicilio, anche in assenza del perpetrarsi di un'attività criminale.

In altri termini, occorreva stabilire se la normativa in materia consentisse di disporre, in relazioni per delitti di criminalità organizzata, l'intercettazione per mezzo di captatore informatico, prescindendosi dall'indicazione dei luoghi in cui questa dovesse avvenire, posta l'impossibilità di una preventiva individuazione dei punti di interesse, data la natura itinerante dello strumento di indagine adoperato. Dunque di superare il problema del domicilio.

Al di là del principio di diritto a cui le Sezioni unite sono addivenute, che ha dichiarato legittimo l'utilizzo del captatore informativo, muovendo da un esame approfondito delle intenzioni del Legislatore perpetrarsi di un'attività criminale.

In altri termini, occorreva stabilire se la normativa in materia consentisse di disporre, in relazioni a indagini a provvedere a un adeguamento normativo che fosse parametrato allo sviluppo tecnologico raggiunto e che, dunque, ampliasse il sistema delle intercettazioni, mediante l'utilizzo dei programmi informatici che consentono l'accesso da remoto ai computer; ciò che rileva è l'inserimento dei programmi di cui si discute, nel novero degli strumenti assoggettati alla disciplina delle intercettazioni, in assenza, tuttavia, di un'espressa definizione del "software" quale elemento da farsi rientrare nella nozione di "apparecchiatura o strumento".

4. INTERCETTAZIONI E *TROJAN*: IL D.LG. 29 DICEMBRE 2017, N. 216 E L. N. 3/2019

Il d.lg. 29 dicembre 2017, n. 216, pubblicato in *Gazzetta ufficiale* l'11 gennaio 2018, ha da un lato introdotto una nuova e complessa disciplina finalizzata alla tutela della riservatezza, con la puntuale previsione di un rinnovato meccanismo di acquisizione delle captazioni al fascicolo delle indagini e l'introduzione dell'archivio riservato per la conservazione dei verbali e delle registrazioni; ma, soprattutto, ha disciplinato per la prima volta l'utilizzo del captatore informatico; oltre a prevedere un nuovo delitto di diffusione di riprese e registrazioni fraudolente – art. 617-*septies* c.p. –.

Il captatore informatico – cd. *trojan* – è un *malware*, occultamente installato su dispostivi elettronici, frequentemente inoculato sui telefoni cellulari di tipo *smartphone*, che consente, sia di acquisire da remoto tutto il contenuto ivi presente, contatti della rubrica telefonica compresi; sia di intercettare il traffico *email*; sia di attivare la fotocamera o il microfono del dispositivo; sia di geolocalizzarlo, sfruttando il sistema g.p.s.

In altri termini, "l'agente intrusore" ha esteso il raggio d'azione delle intercettazioni a trecentosessanta gradi, consentendo di acquisire le comunicazioni e conversazioni intrattenute mediante applicazioni di instantmessaging (quali ad esempio *whatsapp*, *telegram*, *facebook messenger* o simili); di acquisire quanto viene digitato dall'utilizzatore sulla tastiera (c.d. funzione di *keylogger*); o ancora di acquisire immagini, che ritraggono quanto venga visualizzato sullo schermo del dispositivo, utilizzando una rapida sequenza di *screenshots*, ivi eseguiti automaticamente [7].

Esaminando il *trojan* in ciascuna sua singola funzione, l'oscillazione interpretativa che ha coinvolto dottrina e giurisprudenza, riconduceva, di volta in volta, l'attività svolta o nell'alveo dei mezzi di ricerca della prova o come strumento d'indagine atipico, con evidenti incertezze applicative.

La riforma, dunque, si è resa necessaria proprio a fronte di questo dibattito [8], per regola-

———

[7] Pretti, "*Prime riflessioni a margine della nuova disciplina sulle intercettazioni*", su *Dir. pen. cont.*, 1/18, p. 189 ss.

[8] Quanto ad alcuni contributi dottrinali sul tema, si vedano Parodi, *Intercettazioni telematiche e captatore informatico: quali limiti?*, in *Il penalista.it*, 6 novembre 2017; Peloso, *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo*, in *Dir. pen. cont.*, 1/2017, p. 149 ss.; Pinelli, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di stato"*, in *Dir. pen. cont.*, 4/2017, p. 75 ss.; Giordano, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, *ivi*,

mentare in maniera puntuale la nuova fonte di intercettazione, disciplinando solo uno dei diversi possibili utilizzi del captatore informatico, ovvero quello relativo all'attivazione del microfono, che consente di realizzare intercettazioni tra presenti, peraltro limitatamente ai casi di inoculazione del virus su dispositivi elettronici portatili.

Le modifiche apportate all'art. 266 c.p.p. riguardano, da un lato, l'espresso riferimento al captatore informatico, quale ulteriore e legittimo strumento di intercettazione nei procedimenti che concernono i reati indicati al comma 1 della disposizione normativa; dall'altro, la puntualizzazione, al comma 2-*bis*, che l'utilizzo dell'agente intrusore per intercettare le comunicazioni tra presenti è sempre consentito nei procedimenti per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*.

Per quanto riguarda i delitti diversi da quelli di criminalità organizzata, l'intercettazione ambientale con captatore informatico è ammessa, ma nei luoghi di privata dimora è necessario che vi sia il fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa, ai sensi dell'art. 266, comma 2, c.p.p.

L'art. 4 d.lg. n. 216/2017 ha altresì modificato il contenuto del decreto autorizzativo di cui all'art. 267 c.p.p., prevedendo che il Giudice debba indicare, oltre ai gravi indizi, le ragioni di indispensabilità del captatore per lo svolgimento delle indagini. Solo nel caso in cui si proceda per delitti diversi da quelli di criminalità organizzata, il decreto autorizzativo dovrà anche precisare il tempo e il luogo in relazione ai quali è consentita l'attivazione del microfono; mentre per i delitti indicati dall'art. 51, commi 3-*bis* e 3-*quater*, c.p.p., il pubblico ministero può autonomamente disporre l'intercettazione mediante captatore informatico in via d'urgenza, se l'attesa del provvedimento autorizzativo comporti un pregiudizio alle indagini.

I programmi informatici adoperabili per le operazioni di intercettazione devono possedere requisiti tecnici specifici, l'art. 5 del decreto legislativo ha introdotto il comma 2-*bis* nel *corpus* dell'art. 89 disp. att. c.p.p., consentendone l'impiego solo se conformi alle indicazioni stabilite con decreto del Ministero della giustizia.

Con la l. n. 3/2019 – cd spazzacorrotti –, il Legislatore ha inserito tra i delitti indicati dall'art. 266, comma 2-*bis*, c.p.p., i delitti previsti dall'art. 51, commi 3-*bis* e *quater* c.p.p., anche i più gravi reati commessi dal pubblico ufficiale contro la pubblica amministrazione, puniti con la reclusione non inferiore nel massimo a cinque anni, al fine di rafforzare gli strumenti investigativi per contrastarli, prevedendo la possibilità di utilizzare il captatore informatico per intercettare comunicazioni tra presenti.

Dunque, in punto di decreti autorizzativi, le novelle legislative intervenute individuano tre differenti regimi [9], sia nei presupposti ché nel contenuto del provvedimento, in relazione al reato per il quale si procede.

In materia di pubblica amministrazione, infatti, se da un lato il Giudice, in sede di decreto autorizzativo, ha l'onere di indicare il tempo e il luogo rispetto ai quali è consentita l'attivazione del microfono, come è disposto per i reati comuni; dall'altro, invece, abrogando il comma 2 dell'art. 6 d.lg. n. 216/2017, se ne è legittimato l'utilizzo anche nei luoghi di privata dimora,

———

3/2017, p. 177 ss.; Lasagni, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, *ivi*, 7 ottobre 2016; Lorenzetto, *Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico"*, *ivi*, 24 marzo 2016; Cajani, *Odissea del captatore informatico*, in *questa rivista*, fasc. 11, 2016, p. 4140; Balsamo, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *questa rivista*, 2016, p. 2274.

[9] Brunelli, *intercettazioni mediante il captatore informatico: slalom tra differenti regimi autorizzativi e tra norme vigenti e norme non ancora in vigore*, in *Unicost*, 30 maggio 2019

senza alcuna necessità che vi sia il fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa, come previsto dall'art. 4 d.lg. n. 216/2017, per i delitti di cui all'art. 51, commi 3-*bis* e *quater*, c.p.p.

La durata delle intercettazioni è di quaranta giorni, prorogabile di venti giorni, per i periodi successivi, anche in via d'urgenza, da parte del pubblico ministero.

L'art. 7 del decreto legislativo ha previsto che con decreto del Ministro della giustizia [10], da emanare entro trenta giorni dalla data di entrata in vigore, siano stabiliti i requisiti tecnici dei programmi informatici, funzionali all'esecuzione delle intercettazioni, mediante inserimento di captatore informatico su dispositivo elettronico portatile, stabiliti secondo misure idonee di affidabilità, sicurezza ed efficacia, che ne garantiscano un utilizzo entro i limiti di quanto espressamente autorizzato. Tuttavia, la continua evoluzione dei programmi di aggiornamento degli *smartphone* rende inevitabilmente sempre più complessa l'attività di adeguamento dei virus attivati per le operazioni di intercettazione [11].

Nonostante il Ministero della Giustizia abbia assunto l'impegno di organizzare un piano di rafforzamento infrastrutturale, con l'acquisto e l'installazione di apparati server in tecnologia iperconvergente presso le sale adibite delle Procure della Repubblica, con lo sviluppo di un *software* per la ricezione efficiente delle conversazioni, attraverso un rinnovato sistema di controllo delle attività operate dai fornitori esterni [12], in vista della creazione di una rete protetta per le operazioni di intercettazione, la Legge di bilancio 2019 (legge n. 145/2018 in *G.U.* n. 302 del 31 dicembre 2018, suppl. ord. n. 62) ha nuovamente prorogato l'entrata in vigore della riforma "Orlando" sulle intercettazioni, compresa la norma sulla disciplina restrittiva dell'utilizzo dei *trojan* a fini di indagine, all'agosto 2019 [13].

Attualmente, la normativa applicabile, qualora si volesse ricorrere alle intercettazioni di comunicazioni tra presenti mediante captatore informatico, è costituita dagli artt. 266 e 267 c.p.p.

———

[10] Particolare attenzione è stata poi riposta in relazione ai programmi informatici da utilizzare e alle procedure atte all'installazione e alla rimozione dell'intrusore dal dispositivo elettronico portatile. I nuovi commi 2-*bis* ss. introdotti nell'art. 89 disp. att. c.p.p. prevedono che, ai fini dell'installazione e dell'intercettazione attraverso captatore informatico in dispositivi elettronici portatili, possano essere impiegati soltanto programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia. La tematica non è disciplinata dal codice e la giurisprudenza è dovuta intervenire in materia per ribadire che la collocazione delle apparecchiature in luoghi di privata dimora deve ritenersi implicitamente ammessa nel provvedimento che ha disposto l'intercettazione e che il pubblico ministero non è tenuto a precisare le modalità di intrusione (cfr. Sez. II, 13 febbraio 2013, n. 21644, in *C.E.D. Cass.*, n. 255541; Id., 23 ottobre 2012, n. 44936, *ivi*, n. 254116; Id., 25 settembre 2012, n. 41514, *ivi*, n. 253805; Id., 31 gennaio 2011, n. 14547, *ivi*, n. 250032; Id., 2 ottobre 2007, n. 38716, *ivi*, n. 238108; Id., 9 dicembre 2003, n. 24539, *ivi*, n. 230097).

[11] Sul punto cfr l'art. 1, comma 84, lett. *e*), n. 5) della legge delega n. 103/2017, in cui il Legislatore affronta il tema della rapida evoluzione che interessa la materia.

[12] In proposito, Sez. un., 26 giugno 2008, n. 36359, *ivi*, n. 240395 opera la distinzione tra captazione, che avviene necessariamente al di fuori dei locali della procura; e registrazione, unica attività che invece deve svolgersi negli uffici del pubblico ministero a pena di inutilizzabilità delle comunicazioni o conversazioni acquisite ai sensi dell'art. 271, comma 1, c.p.p.

[13] La riforma infatti prevede che tali intercettazioni siano consentite nei luoghi di privata dimora solo quando vi è fondato motivo di ritenere che ivi si stia svolgendo un'attività criminosa (tranne che in caso di dei gravi delitti previsti dagli artt. 51, comma 3-*bis* e comma 3-*quater* c.p.p.). E dispone che pm e giudice debbano motivare l'esigenza di impiego di questa modalità e indicare in quali luoghi e tempi sarà possibile attivare il microfono. Segnaliamo per converso che la legge "spazza-corrotti" ammette sempre le intercettazioni mediante l'uso dei captatori informatici (cd. *trojan*) su dispositivi elettronici portatili nei procedimenti per delitti contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni. Inoltre cade il paletto del loro utilizzo domiciliare, che sarà possibile anche quando non vi è motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

nella versione non modificata dall'art. 4 d.l. n. 216/2017, nonché dalle norme di cui alla l. n. 3/2019, unitamente ai principi di diritto fissati dalle Sezioni unite nella sentenza Scurato del 2016.

In altri termini, per i delitti comuni valgono le affermazioni di principio contenute nella parte motiva della sentenza Scurato, che esclude che possa essere impiegato il captatore informatico quale modalità di intercettazione ambientale; mentre per i delitti di criminalità organizzata, ne è sempre consentito l'impiego e il regime autorizzativo soggiace solo alla necessità della presenza di sufficienti indizi di reato e di una riconosciuta esigenza, ai fini dello svolgimento delle indagini.

5. IL FENOMENO DEGLI *SPY-SOFTWARE* E LE TUTELE PER LA COMMERCIALIZZAZIONE, TRA CAUTELE PER CHI ACQUISTA, VIOLAZIONI DELLA *PRICACY* E *SOCIAL NETWORK*

L'attuale contesto sociale evidenzia una sensibile estensione della sfera intima individuale: social *network* e *smartphone* sono la più eloquente dimostrazione della portata globale del fenomeno che, incidendo profondamente nella nostra concezione di riservatezza, ne ha ridisegnato i confini.

La costante frequentazione del nuovo mondo virtuale lascia tracce costantemente captate, raccolte e archiviate, consente indagini di mercato e monitora consensi politici. La rete diffonde e rende disponibili applicazioni dedicate a carpire informazioni di terzi e, in questo gioco di ruolo che il sistema internet ha messo in moto, ognuno può vestire alternativamente la parte della spia oppure quella della vittima.

Gli "*spy-software*" consentono di svolgere al privato molteplici operazioni che, partendo dalle indagini del datore di lavoro sul dipendente, approdano facilmente all'hackeraggio professionale. Sono utilizzate dal marito che sospetta della moglie o viceversa; come anche necessarie per fini aziendali, studiando la concorrenza di mercato. Sono adoperati per le indagini penali, ma anche proposte al genitore che si preoccupi della vita virtuale del figlio minorenne.

La macchina dell'industria informatica globale, che avanza spedita nel distribuire prodotti formidabili nel settore e che ha modellato l'interesse degli utenti sulle sue infinite possibilità di ricerca e informazione, elargisce prodotti senza fornire istruzioni adeguate, né pone limiti all'utilizzo delle applicazioni in commercio, nonostante la puntualità con cui il Legislatore, attraverso norme che presidino la privacy e la vita privata, ne sanzioni l'utilizzo, al di fuori dei confini interni alla sfera di attinenza individuale.

Scorrendo le pagine *Web* dedicate alla commercializzazione degli "*spy-software*", si intravedono brevi indicazioni circa l'illiceità della captazione e l'uso degli altrui dati, nel caso in cui il software dovesse essere adoperato per sorvegliare un soggetto terzo.

Il successo di mercato dei programmi "spia" si ancora alle sue potenziali utilità, consentendo di accedere a dati rilevanti, la cui conoscenza risulti efficace, al fine di approntare i dovuti interventi e prevenire eventuali problemi di carattere sociale, lavorativo, familiare o assistenziale.

È significativo che la caratteristica più promossa di queste applicazioni sia la garanzia per l'utilizzatore della non rintracciabilità della messa in uso del programma, assicurata dall'operazione in background, che omette dal dispositivo spiato qualsiasi icona relativa al nuovo software istallato. Se ne riscontrano esempi concreti nel programma "*Cerberus*" che, da antifurto per dispositivi mobili e notebook, è stato rapidamente convertito in *spy-software*.

Molti software assicurano, inoltre, il controllo dell'utenza, attraverso il portale dell'applicazione, controllo operabile da qualsiasi pc collegato alla rete.

Il censimento completo delle applicazioni che svolgano attività di intercettazione, nella sua più amplia accezione, non pare attuabile: tra i numerosi *software* commercializzati, si evidenziano "*Wossip Tracker*", "*mSpy*" oppure, "*flexiSPY*", "*howerwatch*", "*Cerberus*, "*iSpyoo*", e ancora, "*Spyzie*", "*SpyBubble*", "*Spyera*", "*The-TruthSpy*", "*Realtime-Spy*", "*Netvizor*", questi ultimi destinati al controllo aziendale, *software* studiati per essere installati direttamente sulle utenze dei dipendenti, da chi dispone delle autorizzazioni di *system administrator* e che non possono essere rilevati dal dipendente, a cui è consentito adoperare l'*hardware* nei limiti e secondo le modalità che sono impostate *ab origine* del datore di lavoro.

Si tratta di forme di controllo installate sul PC e di cui il dipendente viene informato, in grado di monitorare, da remoto, ogni singola attività dallo stesso svolta: dalla digitalizzazione dei caratteri sulla tastiera, alle pagine *Web* visitate e ai tempi di accesso alle stesse, nonché ai file lavorati, aperti e agli applicativi adoperati.

Nel florido mercato degli "*spy-software*" sono state create applicazioni capaci di controllare l'attività sui social network, i tempi di connessione, la messaggistica e, ovviamente, le *chat*, prima tra tutte, tenuto conto della sua diffusione su larga scala, *WhatsApp* – "*Wossip Tracker*" ne è un esempio – e, nonostante le stringenti forme di criptazione, è possibile monitorarne l'utilizzo e le attività compiute dall'utente.

I "*trojans*", di fatto, sono a disposizione di chiunque frequenti la rete, sotto forma di applicazioni create al preciso e manifesto scopo di intercettare i dispositivi cellulari, muniti di sistemi che registrano e filmano l'ambiente in cui si trova il dispositivo, scattando fotografie all'utente tramite la fotocamera del cellulare.

Il *trojan* può essere installato all'interno del dispositivo bersaglio, sia da remoto attraverso l'invio del virus, dissimulato sotto forma di sms, *e-mail* o applicazione di aggiornamento, che è scaricato e installato inconsapevolmente dall'utente (a cui appare come *file* innocuo), sia inserendo manualmente il programma per il controllo a distanza sul dispositivo da controllare (in questo caso l'agente deve avere la disponibilità materiale del terminale) [14].

L'intercettazione telefonica rappresenta una delle funzionalità di base nel caso di "*spy-software*", consentendo il controllo dell'intero traffico delle conversazioni in entrata e in uscita, in modo occulto, veicolando le registrazioni a un server anonimo, attraverso l'utilizzo della connessione dati del dispositivo telefonico.

Vi sono *software* che consentono di ascoltare solo la parte di conversazione relativa al soggetto spiato e nuovi programmi che, invece, consentono di avere un ascolto totale della conversazione, sia quanto al soggetto spiato, che al suo interlocutore: "*FlexiSpy*", consente di attivare da remoto il microfono del telefonino, al fine di registrare le conversazioni con possibilità di conservare la digitalizzazione dei tasti, accedere agli SMS e alle *e-mail*, nonché di eseguire, sempre da remoto, degli *screenshot* delle applicazioni in esecuzione sul dispositivo, trasformandolo in un microfono capace di captare il contesto ambientale in cui questo si trova.

Assolve, tra gli altri, questa funzione "*Spyera*", che attiva l'intercettazione ambientale e il sistema di monitoraggio, anche cronologico, della localizzazione geografica, attraverso l'accesso dal Web oppure inoculandola direttamente sul dispositivo intercettato.

Esaminando le funzioni connesse ai programmi in questione, ulteriore menzione merita la capacità di accedere ai dati, conservarli, programmare le registrazioni e ricevere file audio o

———

[14] Cuomo, *Prova scientifica e processo penale*, p. 726, Cedam, 2017.

video in tempo reale, o programmare la registrazione di una conversazione, come anche la durata della stessa o l'attivazione della fotocamera su cellulare intercettato.

6. CONCLUSIONE

L'elenco dei programmi che sono stati testé citati rappresenta solo una minima parte di quelli attualmente in commercio, progettati per assolve funzioni che si trovano al confine tra ciò che è lecito e ciò che è, invece, penalmente sanzionabile.

Sotto il profilo legislativo, l'inadeguatezza delle norme in vigore, rende impellente una definizione normativa, per quanto la giurisprudenza negli ultimi anni sia più volte intervenuta a ovviarne le lacune, colmandole con interpretazioni estensive, che rischiano di sconfinare nella analogia.

Esaminando i tratti essenziali del reato, alla luce della sentenza in commento, si evidenzia in primo luogo una discrasia tra il momento consumativo del delitto, che dovrebbe coincidere con l'istallazione del programma, che è la condotta tipica indicata dalla norma, e le applicazioni "*spy-software*", la cui concreta azione captativa sovente non necessita di alcuna istallazione, sfuggendo così dal più importante riferimento letterale dell'enunciato normativo.

La finalità descritta all'art. 617-*bis* c.p., intercettare o interrompere le comunicazioni telefoniche, che la Corte di cassazione ha costantemente dichiarato irrilevante per la configurazione del reato, degradandola a mero post factum pare, invece, essere elemento determinante, in quanto questi programmi sono capaci di svolgere più funzioni e, tra le molteplici potenzialità, anche l'intercettazione. È dunque possibile affermare che alla finalità che si intende raggiungere, debba attribuirsi un ruolo essenziale per l'integrazione della condotta criminosa, in linea con l'intenzione manifestata dal Legislatore di tutelare i fatti prodromici alla lesione del nuovo concetto di riservatezza.

In altri termini, occorre procedere a una riformulazione dell'art. 617-*bis* c.p. e a un contestuale adeguamento normativo a presidio del mercato informatico, la cui offerta è sconfinata in maniera evidente nel cyber crime. Il vuoto normativo incide sulla certezza del diritto.

La categoria "aperta e dinamica" degli "*spy-software*" apre un conflitto tra la globale messa in distribuzione di mezzi che l'industria informatica pone a disposizione dell'utenza di rete e le illecite potenzialità che gli sono insiste e l'utente non ne avverte il disvalore, occultato da pubblicità che ne esaltano le potenzialità e la semplicità nel fruirne.

Senza un censimento degli strumenti o parti di essi che assolvano la funzione di intercettare, censimento che il Legislatore del 1978 aveva previsto all'art. 9, ma che di fatto è stato superato dalla giurisprudenza per far fronte all'avvento di sistemi costantemente aggiornati, il delitto enunciato all'art. 617-*bis* c.p., così come attualmente formulato, è privo di attualità e di determinatezza.

Non può peraltro omettersi di rilevare come la sentenza Scurato non si sia pronunziata sulla natura del "*software*" quale elemento rientrante nel novero degli "strumenti o apparecchiature", come già testé è stato rappresentato. In altri termini, l'interpretazione offerta dalla V sezione della suprema Corte pare estendersi oltre al significato letterale della norma, fino a sconfinare nell'analogia *in malam partem*, soprattutto se si considera che, mentre il complesso organico di elementi fisici, che potrebbero legittimamente rientrare nel concetto di "strumento", sono rappresentati, nei sistemi informatici, dal "*hardware*"; il "*software*", invece, ne rappresenta il complesso organico degli elementi astratti, che compongono un apparato di elaborazione dati.

Giurisprudenza richiamata in nota

Sez. V, 18 marzo 2003, n. 12698, in *C.E.D. Cass*., n. 731;
Sez. II, 9 dicembre 2003, n. 24539, *ivi*, n. 230097;
Sez. II, 2 ottobre 2007, n. 38716, *ivi*, n. 238108;
Sez. un., 26 giugno 2008, n. 36359, *ivi*, n. 240395;
Sez. II, 3 ottobre 2008, n. 37710/2008, *ivi*, n. 241456;
Sez. V, 3 ottobre 2008, n. 37710, *ivi*, n. 241456;
Sez. V, 27 gennaio 2011, n. 3061, *ivi*, n. 249508;
Sez. II, 31 gennaio 2011, n. 14547, ivi, n. 250032;
Sez. II, 23 ottobre 2012, n. 44936, *ivi*, n. 254116;
Sez. II, 25 settembre 2012, n. 41514, *ivi*, n. 253805;
Sez. II, 13 febbraio 2013, n. 21644, *ivi*, n. 255541;
Sez. V, 16 settembre 2015, n. 37557, *ivi*, n. 265789;
Sez. un., 1° luglio 2016, n. 26889, *ivi*, n. 266905;
Sez. V, 30 agosto 2018, *ivi*, n. 273768.

Riferimenti bibliografici

Balsamo, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *questa rivista*, 2016, p. 2274.
Brunelli, *intercettazioni mediante il captatore informatico: slalom tra differenti regimi autorizzativi e tra norme vigenti e norme non ancora in vigore*, in *Unicost*, 30 maggio 2019.
Cajani, *Odissea del captatore informatico*, in *questa rivista*, 2016, p. 4140.
Cuomo, *Prova Scientifica e processo penale*, a cura di Canzio e Lupària, p. 726, Cedam, 2017.
Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsggericht sulla cd. On line durchuchung*, in *Riv. trim. dir. pen. econ*., 3, 2009, p. 679 ss.
Giordano, *Dopo le sezioni unite sul captatore informatico avanzano le nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. pen. cont.*, 3/2017, p. 177.
Lasagni, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in *Dir. pen. cont*., 7 ottobre 2016.
Lorenzetto, *Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico"*, in *Dir. pen. cont*., 24 marzo 2016.
Minotti, in *Guida al diritto*, 3 gennaio 2009, n. 1, p. 93.
Orlandi, *Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Archivio pen. (web)*, 25 luglio 2016.
Parodi, *Intercettazioni telematiche e captatore informatico: quali limiti?*, in *Il penalista.it*, 6 novembre 2017.
Peloso, *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo*, in *Dir. pen. cont.*, 1/2017, p. 149 ss.
Pinelli, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di stato*, in *Dir. pen. cont*., 4/2017, p. 75 ss.
Pretti, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, su *Dir. pen. cont*., 1/18, p. 189 ss.

www.giuffre.it/riviste/penale