I sistemi di controllo da remoto nella legislazione interna e sovranazionale

di Wanda Nocerino

Abstract: *Remote control systems in internal and supranational legislation* – The essay examines the internal and European legislative innovations (in particular, Germany, France, England) regarding investigations carried out using the Trojan virus. After highlighting the criticalities of existing regulations, the research continues by analyzing the forms of international and European cooperation for the acquisition of computer data obtained through the computer sensor. The outcome of the study does not seem to lead to comforting results, leaning towards the unusability of the acquired results in the absence of adequate rules governing such particularly invasive activities in full compliance with the legal reserve.

Keywords: Computer sensor; Investigative tools; Interception; Cooperation.

1. Il captatore informatico quale tecnica di "indagine speciale" da remoto

Il tema delle investigazioni tramite captatore informatico continua a fare rumore nel panorama giuridico nazionale e internazionale: nonostante la più o meno recente tipizzazione legislativa sia sul fronte interno che europeo, rimangono ancora vivi i dubbi e le perplessità che attanagliano l'istituto.

Tutti gli "addetti ai lavori" – legislatore, dottrina e giurisprudenza, ciascuno per il proprio àmbito di competenza – si sono interrogati a lungo sulla portata e sui limiti di impiego del *virus* informatico nelle attività investigative, contribuendo a tratteggiare la fisionomia e il ruolo che il *Trojan* assume nel circuito processuale interno e sovranazionale.

Nonostante la ricchezza dei contributi offerti, l'argomento sembra avere ancora contorni poco nitidi, richiedendo un attento studio in ragione dell'impatto sui principi costituzionali e sulle categorie probatorie del processo penale.

Ogni analisi giuridica, però, richiede alcune considerazioni di tipo preliminare, utili ad inquadrare lo strumento del captatore informatico nel vasto panorama delle tecniche investigative, così da misurarne la portata (legata alla *performance* "tecnica", al tasso di impiego investigativo e all'allineamento con i nuovi paradigmi d'indagine a livello europeo) e le sue prossime possibili evoluzioni.

DPCE online
ISSN: 2037-6677

Dalla definizione stessa di "captatore elettronico, si possono scorgere tanto le sue caratteristiche tipiche quanto le insidie tecniche e giuridiche di cui è portatore.

Può dirsi che il captatore – che, lo si precisa, non costituisce un "istituto" processuale ma uno strumento con cui dare esecuzione ai (più o meno) tradizionali mezzi di ricerca della prova – è un sistema dissimulato, inoculato da remoto, che, eliminando gli effetti che impediscono la conoscenza della comunicazione o dei dati, permette la intercettazione in chiaro dei contenuti audio video e dei dati scambiati o consente l'intercettazione tra presenti, e raccoglie da remoto le posizioni assunte dall'apparato sul territorio[1].

Nella nozione si scorge la prima prerogativa del *virus*, ossia l'appartenenza ai sistemi di controllo da remoto (c.d. *Remote Control Systems*). È uno strumento di indagine "a distanza", messo a disposizione dall'innovazione tecnologica attraverso macchinari, apparecchiature e dispositivi in grado di eseguire attività, un tempo condotte in presenza e sul luogo dell'indagine, da una postazione remota.

Non è il solo strumento investigativo di tal genere. Si pensi alle più datate microspie, comunemente impiegate per l'esecuzione delle intercettazioni di conversazioni e comunicazioni tra presenti, ai microfoni direzionali, al tracciamento mediante dispositivi di geolocalizzazione (*GPS tracking*), alle sempre più utilizzate videoriprese effettuate dagli organi inquirenti a fini investigativi.

La remotizzazione offre grandi vantaggi alle indagini, in termini di elevata intrusività e potenzialità informativa, oltre che di basso rischio di "*discovery*". Ma non c'è dubbio che tali vantaggi siano stati amplificati, e sempre più lo saranno, dal momento storico che si vive; momento in cui il processo penale, al pari di ogni altro settore della vita, esige che le attività, le comunicazioni, i rapporti, avvengano in modalità remota quale strumento di contenimento dell'epidemia da Covid-19. Il che porta agevolmente a far pensare in via preliminare che, mai come ora, possa farsi strada un'apertura culturale inedita, una sorta di *favor* da parte del legislatore interno ed europeo, della dottrina e della giurisprudenza, verso l'impiego più generalizzato delle indagini a distanza e verso una stabilizzazione di quelle misure emergenziali nate "a tempo", con lo scopo di imprimere un'accelerazione alla macchina giudiziaria[2].

Si potrebbe ritenere che l'attenzione rivolta negli scorsi anni a tutte le forme di investigazione a distanza (nel tentativo di fornire adeguate risposte sotto il profilo della compatibilità degli esiti investigativi con il sistema costituito, ricorrendo molto spesso alla magmatica categoria della prova

[1] Sul versante interno, la definizione si rinviene nel d.m. 2 marzo 2021, n. 247, recante "*Disposizioni per l'individuazione delle prestazioni funzionali alle operazioni di intercettazione e per la determinazione delle relative tariffe*".
[2] In conformità agli obiettivi europei del P.N.R.R. accordati dal Governo italiano con il Consiglio UE.

atipica) arrivi ad assumere direzioni nuove, inclini a riconoscere un'autonomia concettuale e una più solida tenuta rispetto ai tradizionali valori del processo penale.

Ma c'è di più. Estrapolandolo dall'ampia gamma degli strumenti di indagine a distanza, va rimarcata l'ulteriore caratteristica del captatore informatico; quel *quid pluris* che ne fa il prototipo delle tecniche di indagine speciali (TSI)[3], ossia di metodologie investigative non convenzionali che – ormai da qualche tempo – vengono regolamentate (in modo particolare a livello internazionale)[4] per contrastare illeciti rispetto ai quali le esigenze di repressione sono alimentate da un crescente allarme sociale (crimine organizzato, sostanze stupefacenti, corruzione, pedopornografia, terrorismo) ma soprattutto per penetrare nelle moderne organizzazioni criminali che, in determinati settori, si sono manifestate impermeabili agli ordinari mezzi investigativi.

Più concretamente, il captatore informatico rientra nella *species* della sorveglianza elettronica[5] che permette di controllare a distanza gli spostamenti di soggetti non già identificati o individuati con un impiego minimo di personale di polizia e potenzialmente su aree territoriali sconfinate.

In questo caso – a differenza dei tradizionali strumenti di indagine da remoto –, non si intende controllare un'"area" di interesse investigativo o un singolo "individuo" coinvolto (a vario titolo) in un'indagine, ma chiunque e ovunque si muova nel raggio di azione dello strumento, così da operare un monitoraggio penetrante e ubiquitario che non incontra limiti e confini di sorta, incidendo in maniera significativa sul complesso di garanzie inviolabili dell'individuo.

Oltre al *Trojan* ci sono altri strumenti di sorveglianza elettronica. Si pensi ai sofisticati SAPR (sistemi aeromobili a pilotaggio remoto, comunemente definiti droni), muniti di telecamere con funzione di monitoraggio ambientale e controllo delle infrastrutture o anche alle più

[3] Il Comitato dei ministri del Consiglio d'Europa nella Raccomandazione Rec(2005)10 agli Stati membri sulle "special investigation techniques", definisce queste ultime come «techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons». Così Comitato dei ministri del Consiglio d'Europa, *Reccomendation Rec(2005)10 of the Committee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism*, 20 aprile 2005.

[4] Circa l'impiego delle TSI per la prevenzione e il contrasto del crimine organizzato transfrontaliero, cfr. art. 20 della *Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale*, sottoscritta a Palermo il 15 dicembre del 2000, poi ratificata e resa esecutiva in Italia dalla l. 16 marzo 2006, n. 146, in *Gazz. uff.*, 11 aprile 2006, n. 85; nonché l'art. 50 della *Convenzione ONU contro la corruzione*, sottoscritta a Merida il 9 dicembre 2003, ratificata e resa esecutiva dalla l. 3 agosto 2009, n. 116, in *Gazz. uff.*, 14 agosto 2009, n. 188.

[5] Sull'inquadramento del captatore informatico tra le forme di sorveglianza elettronica, per tutti, Working Group on International Cooperation, *International cooperation involving special investigative techniques*, Vienna, July 2020, in *www.unodc.org*.

DPCE online
ISSN: 2037-6677

moderne tecniche di videosorveglianza analitica basata su intelligenza artificiale. Tuttavia, rispetto a queste, il *virus* elettronico si spinge ancora oltre le già penetranti forme di controllo digitale, andando a frugare nella sfera più intima dell'individuo, nell'"io" più profondo, attentando alla stessa psiche di chi viene monitorato. Infatti, se è vero che la libertà della persona ricomprende persino le cose materiali che rappresentano parti fondamentali della sua esistenza, allora tale impostazione deve estendersi in rapporto al telefono cellulare e più in generale ad ogni dispositivo elettronico, tenendo conto dell'uso che ne è comunemente fatto e dei contenuti spiccatamente personali e delicati ad esso affidati.

Va da sè che il *malware*, non solo "tecnica di sorveglianza speciale" ma anche "tecnica di indagine a distanza", presenta delle peculiarità che lo allontanano inesorabilmente dalle più note metodologie di investigazioni speciali e lo rendono un *unicum* tra gli strumenti di indagine esistenti.

In questa cornice concettuale s'innesta l'interesse dello studioso, la cui indagine deve inesorabilmente prendere le mosse dagli aspetti più arditi (perlomeno per il giurista) relativi alla funzionalità del *Trojan*, senza i quali non è dato cogliere a pieno le sue potenzialità.

Senza addentrarsi profondamente nei meandri del più raffinato tecnicismo informatico, può dirsi che il *virus* consente all'inoculante di prendere il pieno possesso della macchina-bersaglio e, di conseguenza, di apprendere una mole in(de)finita di dati e di informazioni che difficilmente potrebbero essere conosciuti (e conoscibili) dagli investigatori ricorrendo alle tecniche di indagine tradizionali, sfruttando la portabilità e l'imperscrutabilità dello strumento.

Tuttavia, la natura camaleontica del *malware*, combinata alla ontologica insofferenza alle predeterminazioni spazio-temporali, ingenerano non pochi dubbi nello studioso circa la compatibilità degli esiti investigativi che ne derivano con il tessuto processuale e il reticolo normativo sovranazionale. In questo caso, il rischio da scongiurare è che le investigazioni da remoto tramite *virus Trojan*, nelle loro plurime sfaccettature funzionali e sistematiche, travalichino i contenuti e le dimensioni legislative dei singoli ordinamenti che ne ospitano una – seppur embrionale – disciplina e i relativi "corredi" interni e sovranazionali.

Il presente contributo affronterà tali aspetti, incentrandosi in modo particolare sulle differenze esistenti tra la normativa nazionale (solo apparentemente più "garantista") e le discipline europee che hanno dato voce alle plurime tecniche di indagine speciale da remoto anche come risposta alle minacce del terrorismo internazionale[6].

[6] Per un complessivo inquadramento della lotta al terrorismo internazionale, v., *amplius*, A. Ligustro, *Sessant'anni dell'Italia all'ONU: per una celebrazione senza retorica*, in *questa Rivista*, fasc. I, 2016, 3 ss.; P. Picone, *L'insostenibile leggerezza dell'art. 51 della Carta dell'ONU*, in *Riv. dir. internaz.*, 2016, 7 ss.; Id., *Unilateralismo e guerra contro l'ISIS*, *ivi*, 2015, 5 ss. Sul versante procedurale, con riguardo al profilo investigativo, *ex plurimis*, R.E. Kostoris–R. Orlandi (a cura di), *Contrasto al terrorismo interno ed internazionale*,

Da un punto di vista strutturale, la ricerca si concentra inizialmente sull'analisi della normativa interna, evidenziando le regole, i limiti e le criticità della disciplina tratteggiata dal legislatore.

Una volta definiti i confini di impiego del *virus* nelle investigazioni interne, l'indagine intende proseguire lungo due direttrici: in chiave comparativa, procedere ad analizzare la regolamentazione delle tecniche di sorveglianza nei sistemi europei, evidenziandone similitudini e differenze rispetto all'ordinamento interno; in secondo luogo, soffermarsi sulle "nuove" indagini transfrontaliere condotte mediante le tecniche di *remote forensics*. In questo senso, la ricerca si prefigge l'ambizioso obiettivo di rintracciare lo strumento di cooperazione più idoneo alla raccolta transnazionale di informazioni, al fine di verificare la sussistenza di una copertura normativa delle attività di ricerca e acquisizione della prova che transita da e verso l'estero.

2. Gli strumenti di sorveglianza in Europa: approcci comparatistici

In Europa si registra in materia una tangibile dissonanza legislativa, brutalmente contraria a quel processo di armonizzazione auspicato dalla Comunità europea sin dalle sue origini. Infatti, se in alcuni ordinamenti giuridici viene introdotta una disciplina più o meno compiuta dei sistemi di *surveillance*, in altri, apparentemente più garantisti (come l'Italia), le tecniche di controllo da remoto non risultano oggetto di una normativa *ad hoc*.

Non si ritiene che tale impostazione possa essere frutto di una causalità: la scelta di normare le tecniche di controllo da remoto, anche in funzione preventiva, è propria di quegli ordinamenti che risultano (più o meno) direttamente colpiti da attacchi terroristici di matrice internazionale per cui, come conseguenza della proclamazione dello stato d'emergenza, viene affievolito il livello di protezione delle garanzie individuali in nome della sicurezza nazionale.

Prima di analizzare lo *status* ordinamentale vigente in alcuni Stati europei simbolo del *framework* normativo in materia di *surveillance*, è opportuno sin d'ora evidenziare che in tutti gli interventi legislativi si riscontrano le medesime carenze regolamentari.

In primis, l'apertura alle attività di intercettazione su larga scala si fonda su basi opache e poco chiare, mancando la specificazione degli elementi o condizioni che giustificano il ricorso alla misura in esame (difetto di tassatività).

Inoltre, nessuna norma prevede l'introduzione di elementi di controllo e supervisione adeguati circa l'esecuzione delle operazioni necessarie per prevenire eventuali abusi (difetto di giurisdizionalità).

Si anticipa sin d'ora che – a più riprese – sia le Corti interne che la

Torino, 2006; R.E. Kostoris–F. Viganò (a cura di), *Il nuovo "pacchetto" antiterrorismo*, Torino, 2015.

DPCE online
ISSN: 2037-6677

Corte EDU sono intervenute per "sedare" le spinte interne di quei Paesi che si mostrano sempre più propensi ad accogliere i sistemi di *surveillance* elettronica in spregio dei *dicta* comunitari in tema di *privacy*.

Può, quindi, affermarsi, senza timore di smentita, che soprattutto il *trend* giurisprudenziale della Corte EDU, in combinazione con le decisioni di incostituzionalità interne, rappresentano gli indici sintomatici del cambiamento di un sistema che, pur non trascurando le esigenze di sicurezza nazionale, si impone di offrire adeguata tutela al diritto alla *privacy* e alla riservatezza informatica.

3. Il virus Trojan nel contesto nazionale

La materia delle intercettazioni mediante captatore informatico rappresenta il frutto di una stratificazione giurisprudenziale e legislativa senza precedenti. Nonostante gli sforzi profusi, le nuove disposizioni trovano compiuta realizzazione solo quattro anni dopo il primo intervento riformatore. Questa vicenda, si è detto, «presenta i tratti del grottesco»[7].

Più precisamente, dopo una disorganica produzione giurisprudenziale tesa a circoscrivere l'impiego del *Trojan* nelle indagini penali riferite ai soli reati più gravi di criminalità organizzata[8], il definitivo ingresso del captatore informatico nel processo penale viene consacrato già nel 2017[9].

Pur se promulgato nel gennaio 2018, il decreto non trova compiuta realizzazione. Dopo una serie di rimbalzi legislativi che ne hanno posposto l'attuazione [10] e di leggi integrative atte a "correggere il tiro" del frettoloso legislatore del 2017 [11], proprio il 31 dicembre del 2019 – nel giorno della sua ipotetica entrata in vigore – il Consiglio dei Ministri modifica la disciplina

[7] L'espressione appartiene a M. Gialuz, *L'emergenza nell'emergenza: il decreto-legge n. 28 del 2020, tra ennesima proroga delle intercettazioni, norme manifesto e "terzo tempo" parlamentare*, in *Sist. pen.*, 1 maggio 2020.
[8] Cass., Sez. Un., 28 aprile 2016, Scurato, in *Cass. pen.* 2016, 3546.
[9] D.lgs. 29 dicembre 2017, n. 216, recante "*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", in *Gazz. uff.*, 11 gennaio 2018, n. 8.
[10] Ad eccezione di alcune disposizioni dotate di efficacia immediata (art. 6, d.lgs. n. 216/2017), l'applicazione della normativa introdotta dal d.lgs. n. 216/2017, prevista inizialmente per il 26 luglio 2018 (*ex* art. 9, comma 1, d.lgs. n. 216/2017), ha subito una serie di "rimbalzi" legislativi. La data prevista per il 31 marzo 2019 (art. 2, d.l. 25 luglio 2018, n. 91, convertito, con modificazioni, dalla legge 21 settembre 2018, n. 108), è stata prorogata al 31 luglio 2019 (art. 1, comma 1139, lett. *a*), legge 30 dicembre 2018, n. 145) e poi rinviata al 31 dicembre 2019 (art. 9, comma 2, lett. *a*), d.l. 14 giugno 2019, n. 53, convertito, con modificazioni, dalla legge 8 agosto 2019, n. 77).
[11] Ci si riferisce alla legge 9 gennaio 2019, n. 3 (c.d. legge spazza-corrotti), recante *Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*, in *Gazz. uff.*, 16 gennaio 2019, n. 13.

ivi contenuta [12], disponendo un ulteriore differimento dell'efficacia delle disposizioni introdotte, prima al 29 febbraio 2020 [13], poi al 30 aprile 2020 [14], e, infine, al 31 agosto 2020[15], con lo scopo di «consentire il completamento delle complesse misure organizzative in atto, anche relative alla predisposizione di apparati elettronici e digitali» [16].

Al di là dei profili temporali, può evidenziarsi che l'inserto legislativo – attraverso una modifica del comma 2 dell'art. 266 c.p.p. – mira a formalizzare l'istituzione di una nuova tecnica di intercettazione tra presenti da condurre mediante l'immissione di captatori informatici in dispositivi elettronici portatili, attribuendo all'attività in esame uno specifico volto: non una nuova forma di intercettazione, da collocarsi accanto a quelle telefoniche, ambientali e telematiche, ma solo un nuovo strumento attraverso cui espletare un "vecchio" mezzo di ricerca della prova, ovvero per condurre intercettazioni ambientali.

Inoltre, normativizzando il c.d. "doppio binario investigativo" [17] attraverso l'innesto di un inedito comma 2 *bis* all'art. 266 c.p.p., si prevede che tali forme intercettive sono sempre consentite nei luoghi di privata dimora (art. 614 c.p.), a prescindere dalla sussistenza del fondato motivo di ritenere che in quel luogo si stia svolgendo un'attività criminosa, solo nel caso di delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. e per i reati "gravi" contro la pubblica amministrazione[18], previa indicazione delle ragioni che giustificano l'intrusione.

Ulteriori novità si registrano in relazione al contenuto del decreto autorizzativo.

Attraverso un'interpolazione del comma 1 dell'art. 267 c.p.p., si richiede al giudice procedente un ulteriore sforzo documentale per il quale il decreto assumerebbe le vesti di un provvedimento corredato da una motivazione "rafforzata". Infatti, il giudice è sempre tenuto ad indicare la ragioni (specifiche, *ex* art. 2, leggi di conversione del d.l. 30 settembre 2021, n. 132) che rendono necessaria la peculiare modalità operativa, valorizzando

[12] D.l. 30 dicembre 2019, n. 161, recante *Disposizioni urgenti in materia di intercettazioni*, in *Gazz. uff.*, 31 dicembre 2019, n. 305, convertito, con modificazioni, in l. 28 febbraio 2020, n 7.
[13] Art. 1, comma 1, punto 1, del d.l. n. 161/2019.
[14] Legge n. 7/2020, che modifica il comma 1 dell'art. 1 del d.l. n. 161/2019.
[15] D.l. 30 aprile 2020, n. 28, recante "*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*", in *Gazz. uff.*, 30 aprile 2020, n. 111.
[16] Così *Relazione tecnica di accompagnamento al disegno di legge riguardante la conversione del d.l. 161/2019*, reperibile al sito *www.senato.it*.
[17] Art. 13, d.l. 13 maggio 1991, n. 152, convertito, con modificazioni, in legge 12 luglio 1991, n. 203.
[18] Più precisamente, si tratta dei delitti dei pubblici ufficiali e degli incaricati di pubblico servizio contro la pubblica amministrazione, puniti con la reclusione non inferiore nel limite massimo a cinque anni, determinata a norma dell'art. 4 c.p.p.

DPCE online
ISSN: 2037-6677

la concezione per cui il ricorso alle intercettazioni mediante captatore informatico deve essere considerata un'*extrema ratio*.

Ma si badi che la "necessità" indicata nel decreto non equivale al requisito dell'"indispensabilità" del ricorso al particolare strumento investigativo che, per converso, non è richiesto dal dato normativo. Dal tenore letterale della disposizione in esame si evince che non è necessaria la prova del fatto che il ricorso a tale peculiare forma di intercettazione sia l'unico strumento operativo praticabile, dal momento che «il giudizio di necessità non coincide con quello di certa infruttuosità delle altre forme di intercettazione ambientale quanto piuttosto con la prova [...] di una meno agevole praticabilità delle operazioni tradizionali» [19].

Tuttavia, nel caso in cui si proceda per delitti diversi da quelli indicati nell'art. 51, commi 3-*bis* e 3-*quater*, c.p.p., nonchè per quelli "gravi" contro la pubblica amministrazione, gli adempimenti motivazionali si "aggravano" ulteriormente, dovendo il giudice indicare anche «i luoghi e il tempo, anche se indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono» .

Poi, attraverso l'introduzione di un nuovo comma 2-*bis* all'art. 267 c.p.p., il ruolo di protagonista indiscusso del p.m. nell'ambito della procedura d'urgenza viene attenuato: lo stesso, infatti, può procedere ad autorizzare l'esecuzione delle operazioni mediante *virus* informatico con decreto motivato – che dovrà menzionare le specifiche ragioni dell'urgenza, tali da non permettere l'attesa del naturale provvedimento giurisdizionale – solo nel caso in cui si proceda per delitti di criminalità organizzata ed economica richiamati dall'art. 266, comma 2-*bis*, c.p.p. [20].

Da ultimo, le riforme toccano anche la disciplina dei divieti di trasmigrazione dei risultati acquisiti a mezzo *Trojan* in altri procedimenti (art. 270 c.p.p.) e di utilizzazione probatoria dei dati illegittimamente appresi (art. 271 c.p.p.).

Con riferimento al primo aspetto, il legislatore introduce un inedito comma 1-*bis* all'art. 270 c.p.p., statuendo che, fermo restando il divieto di impiego del prodotto delle captazioni in procedimenti diversi da quelli nei quali le stesse sono state disposte [21], «[...] i risultati delle intercettazioni tra

[19] Così D. Pretti, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, in *Dir. pen. cont.*, n. 1, 2018, 219.

[20] Nei casi di cui al comma 2, il pubblico ministero può disporre, con decreto motivato, l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile soltanto nei procedimenti per i delitti di cui all'articolo 51, commi 3-*bis* e 3-*quater*. A tal fine indica, oltre a quanto previsto dal comma 1, ultimo periodo, le ragioni di urgenza che rendono impossibile attendere il provvedimento del giudice. Il decreto è trasmesso al giudice che decide sulla convalida nei termini, con le modalità e gli effetti indicati al comma 2» (comma 2-*bis* dell'art. 267, introdotto *ex* art. 4, comma 1, lett. *b*), punto 2, d.lgs. n. 216/2017).

[21] *Ex* art. 270, comma 1, c.p.p. Con riferimento a tale richiamo, va specificato che tale disposizione subisce una modifica sotto un duplice profilo: da un lato, si rafforzano le condizioni che legittimano l'impiego dei risultati captativi in procedimenti diversi da quelli indicati nel decreto autorizzativo; dall'altro, viene introdotta un'ulteriore ipotesi

presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, se compresi tra quelli indicati dall'articolo 266, comma 2-*bis*» c.p.p.[22], condizionando il loro impiego al canone della "indispensabilità"[23].

Per quanto attiene, invece, al divieto di utilizzazione ultra vis dei dati appresi, attraverso l'interpolazione di un inedito comma 1 *bis* all'art. 271 c.p.p., si statuisce che «[N]on sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo».

Si tratta di una norma destinata a colpire non la mera inosservanza di modalità esecutive ma volta a presidiare alcuni fondamentali confini applicativi dello strumento, benché regolati attraverso cautele operative di natura tecnica.

Al di là degli innumerevoli profili di criticità che possono evidenziarsi nella normativa evidenziata, quello che preme in questa sede evidenziare è la discutibile scelta legislativa – tutta interna – di normare solo una delle molteplici attività che il *malware* è, almeno in potenza, capace di svolgere una volta inoculato sulla macchina-bersaglio, sul rilievo che, attraverso la sola attivazione del microfono del dispositivo elettronico portatile su cui il *virus* agisce, si potrebbero superare le resistenze di chi aveva visto nel captatore una creatura "bulimica"[24] capace di condurre, nello stesso momento, plurime attività. Sul punto, infatti, la dottrina avanza delle riserve[25], ritenendo che «il lato "nascosto", su cui la novella è rimasta silente, crea difficoltà interpretative ancor maggiori di quelle direttamente legate alla lettura del

derogatoria al regime di inutilizzabilità, prevedendo che la trasmigrazione del captato possa considerarsi legittima allorquando risulti «necessaria e indispensabile» non solo per l'accertamento dei delitti per i quali l'arresto in flagranza è obbligatorio, ma anche dei reati di cui all'art. 266, comma 1, c.p.p. Di qui, deve intendersi ristretto notevolmente il divieto di circolazione probatoria dei dati acquisiti a mezzo *Trojan* che, allo stato, può avvenire in procedimenti diversi con riferimento non solo ai reati per cui è previsto l'arresto obbligatorio in flagranza, ma anche a quello di cui all'art. 266, comma 1, c.p.p., nonché per la prova di reati diversi sempre che rientrino tra quelli contemplati nel comma 2-*bis* dell'art. 266 c.p.p.

[22] Cfr. art. 2, comma 1, lett. *g*), punto 1, d.l. n. 161/2019.

[23] Legge n. 7/2020, che modifica l'art. 2, comma 1, lett. *g*), d.l. n. 161/2019.

[24] La definisce così L. Filippi, *L'ispe-perqui-intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi ma sbagliano la terapia*, in *Arch. pen.*, 2016, f. 2, p. 350.

[25] G. Spangher, *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, in *Giur. pen.* web, n. 1, 2018. La scelta limitativa è altresì criticata da P. Bronzo, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in G. Giostra-R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, 237 s., nonché da anche G. Pestelli, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, in *Sist. pen.*, 2020, f. 1, p. 150, per cui l'impostazione è «minimalista e riduttiva».

DPCE online
ISSN: 2037-6677

testo» [26].

L'assenza di qualsivoglia disciplina relativa all'uso del captatore, oltre la semplice attivazione del microfono, creerebbe una "zona grigia" che gli interpreti sarebbero chiamati ad "illuminare", lasciando «alle procure e alla giurisprudenza il compito di definire modalità, regole, effetti dell'uso del captatore per le attività di ispezione, perquisizione e sequestro e quant'altro è possibile acquisire con lo strumento *de quo*» [27].

4. L'esperienza tedesca...

Tra i Paesi europei che adottano una normativa *ad hoc* per disciplinare l'uso dei sistemi di controllo da remoto – soprattutto in fase preventiva – spiccano la Germania e la Francia, in quanto Stati "pionieri" nella legalizzazione dei *software Trojan* ancor prima della minaccia terroristica[28].

Al fine di comprendere più correttamente il "tenore" delle riforme, occorre partire da un rapido *excursus* circa l'impianto legislativo previgente.

Per quanto concerne l'ordinamento tedesco[29] (improntato al principio di ricerca della verità materiale nella sua dimensione ampia di regola comune all'attività investigativa e probatoria, *ex* § 155, 244 comma 2 StPO), l'inviolabilità del segreto della corrispondenza e delle telecomunicazioni è tutelata dall'art. 10 della Legge fondamentale (*Grundgesetz*); l'interferenza al godimento del diritto *de qua* viene, tuttavia, espressamente consentita dagli artt. 100 a) e 100 b) del *Strafprozeßordnung* (StPO), in relazione alle intercettazioni processuali. Con riguardo alle captazioni preventive, la legge sulla limitazione del segreto epistolare, postale e delle telecomunicazioni del 2001[30], legittima le intercettazioni esperite anche in assenza di un procedimento penale.

Con riferimento all'uso del captatore informatico, nel 2006, l'art. 5, comma 2, n. 11 della Legge sulla protezione della Costituzione del Nord Reno-Westfalia consente ad un organismo di *intelligence* di delegazione governativa il monitoraggio e l'accesso a sistemi informatici collegati in Rete per intercettare in modo occulto dati e comunicazioni tramite strumenti tecnici di captazione.

Poi, nel 2008[31], il legislatore federale tedesco introduce nuove

[26] L'espressione appartiene a L. Parlato, *Le perquisizioni* on-line*: un tema che resta un tabù*, in G. Giostra-R. Orlandi (a cura di), *Revisioni normative in tema di intercettazioni. Riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2021, 290.
[27] G. Spangher, *Critiche. Certezze. Perplessità*, cit., 2.
[28] C. 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.*, 2017, f. 1, 149.
[29] T. Rafaraci, voce *Processo penale tedesco*, in *Enc. dir.*, II, 2008, 831 ss.
[30] *Gesetz zur Beschränkung des Brief–, Post– und Fernmeldegeheimnisses*, del 26 giugno 2001
[31] Cfr. §20 (a)-20(x) della sottosezione della legge federale denominata *Bundeskriminalalamtgesetz* (BKAG) del 25 dicembre 2008.

disposizioni finalizzate a consentire investigazioni mediante l'impiego di mezzi informatici che permettono l'acquisizione dei dati da remoto.

In un contesto come quello descritto – che sembra legalizzare *tout court* l'attività captativa *ante* e *post delictum* mediante strumenti tecnici di sorveglianza e monitoraggio – assume un ruolo centrale la giurisprudenza costituzionale che, già a partire dal 2008, si interroga circa la possibilità di ammettere strumenti tecnici di sorveglianza da remoto.

In quella circostanza, la Corte, pur dichiarando la suddetta normativa incostituzionale, non rispettosa dei principi di proporzionalità e determinatezza, non esclude in assoluto l'ammissibilità di strumenti tecnici di indagine, ritenendo, tuttavia, opportuno predisporre una tutela ulteriore e sussidiaria rispetto a quella già vigente.

Di conseguenza, le operazioni investigative suscettibili di comprimere tale nuovo diritto della personalità (proiezione diretta della nuova realtà digitale) possono essere giustificate, non solo da finalità di repressione di reati, ma anche da finalità preventive, a condizione che siano rispettati il principio di proporzionalità e la riserva di giurisdizione[32].

Più di recente, investita della questione, la Corte assume toni più severi, dichiarando l'incostituzionalità di alcune disposizioni della legge federale denominata "*Bundeskriminalamtgesetz*", che disciplina i compiti e l'attività della forza di polizia federale (*Bundeskriminalamt*) e la cooperazione in materia penale tra i Governi statali e quello federale e con i Paesi terzi. Sulla stessa scia della pronuncia del 2008, il *Bundesverfassungsgericht* riconosce in capo al legislatore il dovere di effettuare un bilanciamento tra la protezione che lo Stato deve accordare ai cittadini e i diritti fondamentali vantati dagli stessi, statuendo che tale bilanciamento deve essere condotto nel rispetto del principio di proporzionalità, in base al quale «i poteri investigativi che incidono in maniera profonda sulla vita privata vanno limitati dalla legge alla tutela di interessi sufficientemente rilevanti nei casi in cui sia prevedibile un pericolo sufficientemente specifico a detti interessi»[33].

Nonostante il tentativo di frenare l'uso indiscriminato di strumenti tecnici di monitoraggio tanto in fase preventiva che procedimentale, il

[32] *Bundesverfassungsgericht*, 2 marzo 2010 (1 BvR 256/08, 1 BvR 263/08; 1 BvR 586/08), disponibile al sito *http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html*. Per commenti, R. Flor, *Brevi riflessioni a margine della sentenza* Bundesverfassungsgericht *sulla c.d.* online Durchsuchung. *La prospettiva delle investigazioni ad alto contenuto tecnologico e il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, cit., 349 ss.; Id., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del* Bundesverfassungsgericht: *la decisione del 27 febbraio 2008 sulle* Online Durchsuchung *e la sua portata alla luce della sentenza del 2 marzo 2010 sul* data retention, in *Cyberspazio e diritto*, 2010, 359 ss.

[33] *Bundersverfassungsgericht*, 20 aprile 2016, 1 BVR 966/09, 1 BVR 1140/09. In dottrina, L. Giordano–A. Venegoni, *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *Dir. pen. cont.*, 8 maggio 2016.

DPCE online
ISSN: 2037-6677

Bundestag, a poco più di due mesi dall'attentato di Monaco, interviene a ridisegnare la simmetria tra alcuni degli elementi essenziali della democrazia tedesca, ossia i rapporti tra libertà e sicurezza, *privacy* e *intelligence*, giustizia, prevenzione e repressione.

In particolare, nell'ottobre 2016 entra in vigore il *Communication Intelligence Gathering Act*[34], per cui l'agenzia per la sicurezza esterna (il *Federal Intelligence Service*, BND) diventa titolare del potere di raccolta e processamento di tutte le comunicazioni dei cittadini o enti stranieri che passano per il maggior nodo d´interscambio Internet di Francoforte per esigenze di contrasto non più soltanto del terrorismo e della criminalità organizzata ma anche per atti a ciò prodromici e, dunque, in presenza del rischio che possa realizzarsi un reato di pericolo astratto, determinando un´anticipazione esponenziale della soglia di intervento statuale[35].

In questo rinnovato contesto, trova terreno fertile il ricorso smisurato alle tecniche si controllo da remoto. Nel 2017, infatti, il Governo tedesco approva degli emendamenti legislativi riguardanti il "*Bundestrojaner*"[36] per permettere alle autorità di installare *software* e decrittografare l'uso privato di Internet senza consenso.

Non solo. Qualche mese (giugno 2021) fa la coalizione di Governo ha raggiunto un accordo sull'uso dei *Trojan* statali sia da parte della polizia federale che del servizio di protezione costituzionale, così da estendere le – già lassiste – regole vigenti nel sistema preventivo anche in quello procedimentale.

5. ...e quella francese

Con riferimento all'ordinamento francese[37], la materia delle intercettazioni è articolata su un doppio binario: da un lato, l'art. 100 del *Code de procédure pénal* relativo ai procedimenti ordinari prevede che sia il *juge d'instruction* a disporre operazioni intercettive in procedimenti per *délits o crimes* puniti con più di due anni di reclusione e per una durata di quattro mesi rinnovabile, dall'altro, a seguito della legge 9 marzo 2004 è possibile disporre intercettazioni preventive sulla base di una disciplina derogatoria prevista dall'art. 706-95 c.p.p. in materia di criminalità organizzata – disciplinata nel libro IV del *Code de procédure* – che consente già durante l'*enquête préliminaire o de flagrance* di ricorrere alle operazioni di intercettazione.

[34] Sul tema, A. Soro, *La legge tedesca sulle intercettazioni che rischia di intaccare le nostre libertà*, in *Guida dir.*, 22 ottobre 2016.
[35] A fronte dell'espresso divieto di fare ricorso a questo tipo di misure per le comunicazioni di cittadini tedeschi, per quelle inerenti i cittadini di altri Stati membri della UE si ammette tale possibilità solo in presenza di indizi di coinvolgimento in attività terroristiche. Cfr. A. Soro, *La legge tedesca sulle intercettazioni che rischia di intaccare le nostre libertà*, in *Guida dir.*, 22 ottobre 2016.
[36] Il *Bundestrojaner* è un *malware* dalle caratteristiche tipo *Trojan*, in circolazione già dal 2011.
[37] G. Aimonetto, voce *Processo penale francese*, in *Enc. dir.*, II, 2008, 723 ss.

Preme evidenziarsi che nell'ordinamento francese si ritrova una disciplina *ad hoc* – già prima delle emergenze terroristiche che hanno sconvolto il Paese – in rapporto all'uso degli strumenti tecnici di captazione. Infatti, l'art. 706-102-1 c.p.p. disciplina la c.d."*captation des données informatiques*" che consente, sempre tramite dispositivo inoculato su un supporto informatico, l'accesso a tutte le informazioni dell'utente *ivi* presenti e il compimento di una serie di attività di salvataggio, stoccaggio e trasmissione di tali dati[38].

Inoltre, la legge n. 731 del 3 giugno 2016 introduce, agli artt. 706-95-4 e seguenti del *Code de procédure pénale*, una specifica disciplina dell'*IMSI Catcher*, altro strumento tecnologico, simile ad un'antenna, che permette di captare e localizzare il numero di telefono e che, nelle versioni più aggiornate, può anche permettere di intercettare dati[39].

Nonostante la predisposizione di un apparato normativo alquanto dettagliato (e, almeno nella forma, garantista) in materia, appena due settimane dopo gli attacchi di Parigi, il Parlamento emana l'*International Electronic Communication Law*[40] con cui si autorizza un'Agenzia esterna di *intelligence* (c.d. *French Directorate General for External Security*) ad intercettare, raccogliere e monitorare le comunicazioni inviate o ricevute all'estero senza necessità di ricevere alcuna autorizzazione giurisdizionale e, conseguentemente, senza precisare i "motivi" dell'ingerenza, ossia le ragioni per le quali la misura sia ritenuta idonea alla salvaguardia della sicurezza collettiva[41].

---

[38] Per una panoramica sulla normativa *de qua*, F. Galli, *The interception of communication in France and Italy – what relevance for the development of English law?*, in *The International Journal of Human Rights*, v. 20, 2016, 666 ss.; C.C. Renard, *Online Surveillance in the Figh Against terrorism in France*, in *Eu Internet Law*, 2018, 385.

[39] Sul punto, C. Peloso, *La scelta della Francia di autorizzarsi a derogare la convenzione europea dei diritti dell'uomo: la portata dell'articolo 15 Cedu nel quadro dello stato di necessità*, in *www.europa.eu*, 15 febbraio 2016; J.F. Renucci, *État d'urgence: la France s'autorise à déroger à la Convention edh*, in *www.lalegislazionepenale.eu*, 21 dicembre 2015. Volendo, v. anche W. Nocerino, *Il tramonto dei mezzi di ricerca della prova nell'era 2.0.*, in *Dir. pen. proc.*, 2021, 1017 ss.

[40] Law 24 July 2015, no 2015–912, *www.legifrance.gouv.fr*.

[41] Il *Conseil constitutionnel* viene chiamato a dichiarare la legittimità della legislazione emergenziale varata a seguito degli attentati terroristici di Parigi del novembre 2015. Con la sentenza n. 536 del 2016, la Corte transalpina, dopo aver ribadito l'astratta legittimità della limitazione imposta alle prerogative dei singoli da parte delle norme scrutinate, in quanto giustificata dalla fondamentale necessità di contrasto alla minaccia terroristica, critica la previsione che consente l'estrazione totale di copia dei dati registrati in apparecchi informatici rinvenuti durante le perquisizioni domiciliari effettuate in forza della legislazione speciale. Si evidenzia, infatti, che la procedura descritta non contemplava alcun intervento preventivo del giudice al fine di autorizzare l'esecuzione della misura, malgrado la considerevole afflittività della stessa anche in quanto suscettibile di incidere sulla sfera giuridica di soggetti diversi dal sospettato. Si censura poi la possibilità di copiare i dati a prescindere dall'esistenza di indizi sufficientemente circostanziati, nonché la mancanza di qualsiasi previsione diretta a regolare il futuro utilizzo delle informazioni raccolte. Tutto ciò conduceva dunque a dichiarare l'incostituzionalità della specifica previsione, appunto perchè sproporzionata rispetto alle finalità di tutela della collettività perseguite. Sul punto, F. Nicolicchia, *Il*

DPCE online
ISSN: 2037-6677

6. L'esperienza inglese e le censure della Corte EDU

In Gran Bretagna, già nel 2000, viene introdotta una normativa *ad hoc* che consente l'uso di strumenti di indagine tecnica per compiere sorveglianza sia in fase preventiva che procedimentale.

La principale fonte normativa in materia di intercettazioni è costituita dal *Regulation of Investigatory Powers Act* 2000 (RIPA), con cui il legislatore, innovando la precedente regolamentazione del 1985, compie una organica revisione dei poteri investigativi delle autorità inquirenti e delle Forze di polizia, resasi necessaria in ragione dell'evoluzione tecnologica e, soprattutto, della diffusione delle comunicazioni elettroniche e dei dispositivi di crittografia. La legge del 2000 disciplina, in particolare, le attività di investigazione il cui esercizio contempli l'intercettazione delle comunicazioni, l'acquisizione dei dati relativi al traffico telefonico, la decrittazione dei dati, il ricorso ad agenti ed informatori. Essa delinea un quadro di garanzie attraverso la delimitazione delle finalità per il legittimo uso di questi strumenti investigativi, l'individuazione dei soggetti abilitati ad avvalersene, la previsione di appositi procedimenti di autorizzazione, il conferimento alla magistratura di compiti di supervisione indipendente e, infine, il riconoscimento alle persone interessate di un diritto di opposizione, a seconda dei casi, all'effettuazione o alla prosecuzione delle attività suddette[42].

In questo contesto, il 29 novembre 2016 viene emanato l'*Investigatory Powers Act* (c.d. Carta di *Snooper*) con cui il Paese, anche in ragione dell'allarme terroristico avvertito negli Stati limitrofi, legittima il ricorso alla sorveglianza massiva con strumenti tecnici quale espediente per la neutralizzazione del fenomeno.

L'intervento legislativo *de quo* si snoda lungo due linee direttrici: da un lato, viene consacrato il diritto per le Agenzie di *intelligence* britanniche (*British Intelligence Community*) di compiere intercettazioni non mirate dei dati e delle comunicazioni; dall'altro, si consente a che le autorità pubbliche possano visionare i *record* relativi alle comunicazioni degli utenti, a prescindere dall'autorizzazione (mandato) dell'autorità giudiziaria[43].

Tuttavia, qualche anno dopo, Corte EDU interviene per censurare la normativa vigente nel Regno Unito, in quanto lesiva del diritto alla riservatezza (art. 8 CEDU) e della libertà di espressione (art. 10 CEDU)[44].

principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova, cit.; S. Scagliarini, *La* privacy *al tempo dell'*état d'urgence: *il* Conseil constitutionnel *sentenzia correttamente*, in *Giur. cost.*, 18 aprile 2016.

[42] Sul sistema penale inglese, V. Patanè, voce *Processo penale inglese*, in *Enc. dir.*, II, 2008, 744 ss.

[43] Per commenti, E. Bassoli, *Uk: approvato l'Investigatory Powers Act*, in *Sic. e giust.*, 2016, 10 ss.; S. Cecinini, *Il Regno Unito e il terrorismo*, cit., 4. Più in generale, per una panoramica sulla legislazione emergenziale inglese, S. Cecinini, *Il Regno Unito e il terrorismo*, in *Sic. internaz.*, 24 settembre 2017.

[44] Corte EDU, 13 settembre 2018, *Big Brother e altri c. Regno Unito*, *applications* n. 58170/13, 62322/14 *and* 24960/15. Nel giudizio promosso da diversi ricorrenti

Secondo la Corte di Strasburgo, «i metodi di raccolta dei dati e la mole di persone tracciate non risultano specificati in maniera sufficiente e [...] mancano regole su filtraggio, ricerca e selezione delle comunicazioni sottoposte a controllo. [....] Raccogliere non solo i dati sul traffico ma anche il contenuto delle comunicazioni che possono essere monitorate costituisce una grave invasione della *privacy*. [...] Il sistema di sorveglianza di massa non è, di per sé, una violazione, ma tale sistema deve rispettare rigidi criteri [...]. Quanto attuato nel Regno Unito, invece, eccede il grado di interferenza che può essere considerato "necessario in una società democratica"».

La pronuncia rappresenta, in sostanza, la pietra miliare di una politica europea tesa al progressivo scardinamento della normazione europea che legittima il ricorso alle tecniche di *surveillance* in assenza di una precisa normazione che delinei tempi, casi e modi dell'ingerenza, nell'ottica di una proporzione tra le esigenze investigative e di prevenzione e la tutela dei diritti fondamentali.

7. Le investigazioni transfrontaliere: il vuoto di tutela nel quadro normativo europeo

Dopo aver analizzato la legislazione nazionale vigente in materia di captazioni tramite *software Trojan* e averla comparata con il quadro normativo di alcuni Paesi europei che si sono dotati di una – seppur scarna – disciplina delle tecniche di controllo per le investigazioni preventive e procedimentali, l'indagine prosegue analizzando (ove esistenti) di strumenti comuni per l'acquisizione delle prove digitali nel cyberspazio.

Va immediatamente precisato che, da diverso tempo, la Comunità internazionale – pur se con qualche resistenza[45] – ha avvertito la necessità di adeguare le forme di cooperazione giudiziaria esistenti allo sviluppo tecnologico, attraverso la previsione di regole uniformi per la raccolta, la

(associazioni e giornalisti attivi nel campo delle libertà civili), la Corte constata l'indebita ingerenza nel diritto alla vita privata costituita dalle attività di intercettazione su vasta scala delle comunicazioni elettroniche e di condivisione dei dati raccolti poste in essere dai servizi segreti del Regno Unito in collaborazione con quelli statunitensi. Sebbene le intercettazioni di massa non siano di per sé incompatibili con la Convenzione, la Corte ravvisa nel caso di specie (riferito all'applicazione delle norme vigenti prima della riforma introdotta con l'*Investigatory Powers Act* 2016) l'insussistenza di adeguate garanzie nelle modalità con cui le autorità ottengono i dati dai fornitori di servizi della comunicazione, lesive anche della libertà di espressione poiché non tutelano le fonti giornalistiche confidenziali.

[45] Come si legge al punto 189 del Rapporto esplicativo alla Raccomandazione n. 13 del 1995 del Consiglio d'Europa, avente a oggetto "*Problemi di diritto penale processuale connessi all'informazione tecnologica*" (Raccomandazione R(95)13 adottata dal Consiglio dei Ministri degli Sati membri del consiglio d'Europa l'11 settembre 1995), la maggioranza degli Stati mostrava grande diffidenza verso modelli di ricerca a livello di *network* effettuata nello Stato dove i dati fossero accessibili o conservati, intendendola come una violazione di sovranità dello Stato, nonché un'evidente deviazione dai passaggi obbligati della mutua assistenza convenzionale che sarebbe stata, così, aggirata.

conservazione e l'utilizzo processuale della *e-evidence*[46].

Si pensi alle innovazioni introdotte dalla Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001[47], oppure, a livello europeo, alla Decisione quadro relativa al mandato di ricerca europeo (MER) del 2008[48], alla Direttiva sull'Ordine Europeo di Indagine del 2014[49], nonchè, da

[46] Cfr. Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione Europea, siglata a Bruxelles il 29 maggio 2000. Più nel dettaglio, negli artt. 10, 11 e da 17 a 22 relativi alle intercettazioni di telecomunicazioni, si fa esplicito riferimento all'obiettivo di tenere conto nel settore della cooperazione giudiziaria anche delle più importanti innovazioni e sviluppi della tecnologia. Sebbene la Convenzione non parli esplicitamente di prove digitali (e in generale nemmeno di prove in forma "tradizionale"), essa rappresenta un documento fondamentale per l'acquisizione transnazionale di prove, dal momento che introduce la possibilità di ricomprendere nella richiesta di cooperazione giudiziale da parte di uno Stato membro anche le *digital evidences*. Per dovere di completezza si precisa la Convenzione è stata ratificata nell'ordinamento nazionale con l. 21 luglio 2016, n. 149, recante "*Ratifica ed esecuzione della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea, fatta a Bruxelles il 29 maggio 2000, e delega al Governo per la sua attuazione*", in *Gazz. uff.*, 27 aprile 2017, n. 97. Con il d.lgs. 5 aprile 2017, n. 52, recante "*Norme di attuazione della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea, fatta a Bruxelles il 29 maggio 2000*", in *Gazz. uff.*, 27 aprile 2017, n. 97, vengono fissate – tra l'altro – le modalità di trasmissione della richiesta di assistenza (art. 7) e l'esecuzione della richiesta di assistenza di uno Stato per attività probatoria (art. 8). In questo contesto, non va sottovalutato il Regolamento per l'istituzione dell'*European Public Prosecutor Office* per la tutela degli interessi finanziari dell'UE, il quale attribuisce a tale Ufficio – tra l'altro – il potere di investigare servendosi delle tecnologie informatiche. Cfr. Art. 30, Regolamento (UE) 2017/1939 del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO»). Sul tema, per tutti, L. Kalb, *Questioni problematiche in tema di Procura europea*, in AA.VV., *Lo spazio di libertà, sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere*, Napoli, 291 ss.

[47] La Convenzione sul *cybercrime* del Consiglio d'Europa, siglata a Budapest il 23 novembre 2001 è stata aperta alle firme in data 23 novembre 2001 ed è entrata in vigore (intervenute le cinque ratifiche previste) il 1 luglio 2004. Si badi che la Convenzione è stata sottoscritta anche da Stati non appartenenti al Consiglio d'Europa, tra cui gli Stati Uniti, il Canada e il Giappone. La Convenzione dedica un secondo gruppo di disposizioni (Capitolo III) alla raccolta transnazionale delle prove digitali, secondo meccanismi di cooperazione che coinvolgono istituti tradizionali o che approdano a forme di collaborazione di nuovo conio, con l'intento di organizzare un sistema internazionale di cooperazione veloce ed efficace. Il trattato è stato ratificato in Italia con la l. 18 marzo 2008, n. 48 recante "*Ratifica della Convenzione del Consiglio d'Europa di Budapest sulla criminalità informatica*", in *Gazz. uff.*, 4 aprile 2008, n. 80.

[48] Decisione quadro n. 978 relativa al mandato europeo di ricerca delle prove del 2008 (MER), diretta all'acquisizione di oggetti, documenti e dati da utilizzare nei procedimenti penali. Al Considerando n. 7 prevede che la Decisione «può essere utilizzata per acquisire, ad esempio, gli oggetti, i documenti o i dati che provengono da un terzo o risultanti dalla perquisizione di locali, *ivi* compresa la perquisizione domiciliare, i dati storici sull'uso di servizi, comprese le operazioni finanziarie, verbali di dichiarazioni, interrogatori e audizioni e altri documenti, compresi i risultati di speciali tecniche investigative». L'ambito di esecuzione, dunque, è limitato alle prove già esistenti, anche di natura digitale.

[49] Direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014 relativa all'Ordine Europeo di Indagine penale, attuata nell'ordinamento nazionale con d.lgs. 21 giugno 2017, n. 108, in *Gazz. Uff.*, 13 luglio 2017, n. 63.

ultimo, alla Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche[50].

A prescindere dalla sussistenza di una (più o meno) solida base normativa[51], continuano ad evidenziarsi criticità in rapporto all'individuazione della "competenza territoriale" della normativa applicabile alla fattispecie concreta[52].

Più nel dettaglio, trattandosi di indagini di tipo *cyber*[53] – per le quali si riscontra «una scissione tra il luogo in cui si trovano i potenziali elementi probatori e il luogo dal quale essi possono essere acquisiti»[54] –, si pongono delicate questioni interpretative e significative preoccupazioni legate all'apprensione e all'utilizzo processuale dei dati archiviati presso *server* esteri[55], ovvero di informazioni che, per loro stessa natura, sono capaci di

[50] Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, COM(2018) 225 final, 17 aprile 2018.

[51] Sottolineano la sussistenza di un pluralismo normativo tutt'altro che sistematico, tra i tanti, M. Daniele, *La vocazione espansiva delle indagini informatica e l'obsolescenza della legge*, in *Proc. pen. giust.*, 2018, 831 ss.; F. Siracusano, *La prova informatica transnazionale*, in *Proc. pen. giust.*, 2017, 178.

[52] Come rileva F. Siracusano, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., 180, «[L]a raccolta transfrontaliera della prova è operazione assai complessa in quanto incline a incidere su due diverse entità: da un canto l'individuo, la cui sfera personale può essere invasa dall'attività di apprensione del dato informativo funzionale all'accertamento giudiziale; dall'altro lo Stato estero, sollecitato a prestare assistenza, la cui sovranità può essere intaccata dall'istanza *lato sensu* probatoria del Paese richiedente cooperazione»

[53] Sulle investigazioni digitali transfrontaliere, *ex multis*, M. Daniele, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in A. Cadoppi-S. Canestrari-A. Manna-M. Papa (a cura di), Cybercrime. *Trattato di diritto penale*, Torino, 2019, 1621 ss.; Id., *La vocazione espansiva delle indagini informatica e l'obsolescenza della legge*, in *Proc. pen. giust.*, 2018, 831 ss.; G. Di Paolo, voce *Prova informatica*, in *Enc. Dir.*, Annali, VI, Milano, 2016, p. 739 ss.; L. Luparia-G. Ziccardi, *Investigazione penale e tecnologia informatica: l'accertamento del reato tra processo scientifico e garanzie fondamentali*, Milano, 2017; M. Pittiruti, Digital evidence *e procedimento penale*, Torino, 2017, p. 2 ss.; S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 161 ss.; Con precipuo riferimento alla tematica delle intercettazioni all'estero, M. Daniele, *Intercettazioni ed indagini informatiche*, in R.E. Kostoris (a cura di), *Manuale di procedura penale europea*, Milano, 2017, III ed., 481 ss.; C. Parodi, *Ordine di indagine europeo: la disciplina delle intercettazioni*, in *Cass. pen.*, 2020, p. 1314 ss.; F. Vergine, *L'elemento della extraterriotorialità*, in T. Bene (a cura di), *L'intercettazione di comunicazioni*, Bari, 2018, 346 ss.

[54] Così S. Signorato, *Le indagini digitali*, cit., 161. Parla di «deterritorializzazione», M. Hildebrandt, *Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace*, in *University of Toronto Law Journal*, 2013, 196 ss. e Ead, *The Virtuality of Territorial Borders*, in *Utrecht Law Review*, 2017, 13 ss. Secondo P. Maggio, *Intercettazioni* no limits: *il captatore informatico "per instradamento"*, in *Proc. pen. giust.*, 2021, 459, le captazioni informatiche determinano una «rarefazione spaziale».

[55] Sul punto F. Cajani, *Le richieste per finalità di giustizia rivolte agli* internet service providers *esteri*, in S. Aterno- F. Cajani-G. Costabile-D. Curtotti (a cura di), Cyber Forensics *e indagini digitali Manuale tecnico-giuridico e casi pratici*, Torino, 2021, 413 ss.; D. Curtotti, *Indagini* hi-tech, *spazio* cyber, *scambi probatori tra Stati e* Internet provider service *e "Vecchia Europa": una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 2021, 745; M. Daniele, *L'acquisizione delle prove digitali dai* service provider: *un preoccupante cambio*

DPCE online
ISSN: 2037-6677

transitare nell'etere digitale attraverso la memorizzazione direttamente sulla Rete, servendosi del c.d. *Cloud*[56].

Proprio in ragione dell'immaterialità e della volatilità dei dati digitali[57], la criticità delle investigazioni *ultra fines* risiede nella individuazione della disciplina da applicare nell'alternativa tra norme appartenenti allo Stato in cui la prova è reperibile (c.d. *lex loci*) e quelle del luogo in cui la prova stessa viene utilizzata (c.d. *lex fori*), anche tenendo conto del coinvolgimento o meno di Paesi estranei all'Unione Europea.

Si può anticipare che, in linea di massima, la normativa vigente in materia di indagini digitali transfrontaliere[58] tende ad adottare le "formalità" e le "procedure" necessarie ai fini dell'utilizzabilità della prova in base alla legge del *locus iudicii*, sempre che essa non sia in conflitto con i principi fondamentali dell'accusato e delle altre persone coinvolte.

Il quadro, già assai convulso, si complica poi quando le attività di investigazione transnazionali si avvalgono di strumenti di investigazioni speciali basati su tecniche di *live forensics*, tra i quali rientra a pieno titolo il captatore informatico.

Come ormai noto, tali congegni informatici funzionanti da remoto sono, per loro stessa natura, refrattari alle circoscrizioni spaziali: di conseguenza, posto che il *virus* rende possibile un ubiquitario del soggetto "attenzionato" e assicura assicurare l'accesso ad una mole enorme di informazioni, soprattutto nell'ultimo tempo, si assiste un uso incondizionato dei *software* tipo *Trojan* nelle indagini che spaziano oltre i confini del territorio dello Stato in cui l'indagine si origina.

In questo contesto, di recente, si è posta la questione legata alla legittimità dell'esecuzione delle operazioni *de quibus* qualora il soggetto

di paradigma nella cooperazione internazionale, in *Rev. Brasileira de Direito Processual Penal*, 2019, 1282 ss.

[56] Sulle questioni legate alla memorizzazione dei dati nel *Cloud*, si rinvia a M. Daniele, *La vocazione espansiva delle indagini informatica e l'obsolescenza della legge*, cit., p. 831 ss.; A. Mangiaracina, *Nuovi scenari nell'accesso transfrontaliero alla prova "elettronica"*, in V. Militello-A. Spena (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Torino, 2018, p. 421 ss.; F. Siracusano, *La prova informatica transnazionale*, cit., 180 s. Sul *cloud computing* quale problematica di diritto internazionale, per tutti, G.M. Ruotolo, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, 87 ss.

[57] Su tali caratteristiche, per tutti, S. Signorato, *Le indagini digitali*, cit., p. 121 ss. Secondo R. Flor, *La Corte di Giustizia considera la Direttiva europea 2006/24 sulla c.d. "*data retention*" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont.*, 2014, f. 2, 190, «l'inarrestabile rivoluzione informatica» e la sua «esasperata velocità evolutiva» abbiano «trasformato i dati e le informazioni in "beni immateriali" di inestimabile valore».

[58] Con riferimento alla rogatoria, si vedano l'art. 4 della Convenzione di assistenza giudiziaria dell'Unione Europea del 2000, l'art. 8 del d.lgs. 5 aprile 2017, n. 53, l'art. 27, comma 3 della Convenzione di Budapest sulla criminalità informatica del 2001 e l'art. 725 c.p.p.; per l'OEI, vedasi l'art. 9, comma 2 della direttiva 2014/41 e gli artt. 4, comma 2 e 5, comma 3 del d.lgs. 21 giugno 2017, n. 108.

monitorato si sposti al di fuori del territorio nazionale[59].

Per comprendere concretamente i termini della questione, si pensi alle ipotesi in cui il captatore viene inoculato sul territorio dello Stato nel corso di un'indagine circoscritta ad una specifica area geografica e, nel prosieguo dell'attività investigativa, il soggetto monitorato si sposta all'estero, utilizzando le stesse utenze per cui viene autorizzata l'intercettazione in Italia[60].

Più precisamente, l'uso del *Trojan* pone non poche difficoltà in rapporto all'accertamento territoriale della captazione, dal momento che difettano le condizioni per prevedere i luoghi (o i mezzi) ove (o mediante i quali) avverranno le attività di investigazione.

Proprio per queste ragioni, è di fondamentale importanza interrogarsi sulle forme di assistenza giudiziaria riconosciute dall'ordinamento interno e sovranazionale, posto che «la cooperazione processuale penale tra gli Stati non può essere limitata a quella tra le loro polizie né finalizzata alla (sola) protezione degli interessi interni, perché questi sono ormai connessi alla protezione degli interessi collettivi di più Paesi»[61].

8. Segue: le acquisizioni "estero su estero"

La prima forma di cooperazione internazionale con cui sembra doveroso confrontarsi è la rogatoria (artt. 727 ss. c.p.p.)[62]. Si tratta di uno strumento di assistenza giudiziaria invocabile – almeno in astratto – ogniqualvolta l'intercettazione (o un'altra attività investigativa) abbia ad oggetto utenze situate in uno Stato *extra*-unionale, ovvero si svolga interamente all'estero.

Al fine di verificare la compatibilità della tecnica di cooperazione

[59] Cfr. G. Illuminati, *Prove*, in G. Conso-V. Grevi-M. Bargis (a cura di), *Compendio di procedura penale*, Padova, 2018, IX ed., 366 ss.

[60] Si precisa che in questa sede non si affronteranno le problematiche relative

[61] Così G. Ubertis, *Considerazioni generali su investigazioni e prove*, in *Cass. pen.*, 2017, 49 ss. D'altra parte, l'esigenza di cooperazione transfrontaliera per facilitare lo scambio informativo tra diversi Paesi emerge con chiarezza dalle Conclusioni del Consiglio europeo del 27 novembre 2008, con le quali si invitavano espressamente gli Stati membri ad agevolare la perquisizione a distanza, al fine di consentire ai servizi investigativi dei diversi Stati di accedere rapidamente alle informazioni e, quindi, ai sistemi informatici, ovunque localizzati, pertanto anche al di fuori dei naturali confini della giurisdizione di uno Stato. Cfr. Considerando *b* della Risoluzione del Parlamento europeo, del 23 ottobre 2013 sulla criminalità organizzata, la corruzione e il riciclaggio di denaro: raccomandazioni in merito ad azioni e iniziative da intraprendere (relazione finale) (2013/2107(INI).

[62] Sull'istituto in esame, senza pretese di completezza, v. AA. VV., *Rogatorie penali e cooperazione giudiziaria internazionale*, Torino, 2003; G. Daraio, *Le rogatorie*, in G. Spangher-A. Marandola-G. Garuti-L. Kalb (diretto da), *Procedura penale. Teoria e pratica del processo*, vol. IV, Torino, 2015, 1155 ss.; G. Della Monica, voce *Rogatorie*, *Diritto* on line *2016*, in *www.treccani.it*. Sull'istituto modificato ad opera del d.lgs. 3 ottobre 2017, n. 149, *ex multis*, G. Di Paolo, *Rogatorie*, in F. Ruggieri (a cura di), *Processo penale e regole europee: atti, diritti, soggetti e decisioni*, Torino, 2018, 125 ss.; Ead., *La riforma della disciplina codicistica delle rogatorie internazionali*, in *Cass. pen.*, 2018, 3431 ss.; F. Ruggieri, *Diritto processuale e pratiche criminali*, Torino, 2018, 543 ss.

DPCE online
ISSN: 2037-6677

predetta con l'intercettazione tramite captatore informatico, occorre innanzitutto soffermarsi sulla fisionomia che l'istituto della rogatoria assume nell'ultimo tempo.

Genericamente, per *ius receptum*, la rogatoria è diventata una forma di cooperazione "residuale" cui ricorrere solo per captare conversazioni e comunicazioni "estero su estero" non transitanti su nodi italiani, ovvero effettuate senza l'ausilio dei c.d. ponti telefonici[63]. Al contrario, quando il traffico telefonico viene captato dall'Italia (a prescindere dal luogo in cui si trova l'utenza), non si delineano i presupposti della rogatoria ma del c.d. instradamento.

Tale tecnica investigativa consente la percezione delle comunicazioni che partono dall'Italia e sono dirette ad un'utenza estera determinata, o ad un fascio di utenze appartenenti ad un distretto geografico di cui fa parte una città situata all'estero, con possibilità di utilizzo simultaneo dei flussi

telematici in luoghi e nazioni diversi ed evidenti sconfinamenti nella percezione dei contenuti comunicativi di soggetti al di fuori della giurisdizione nazionale.

In questi casi, non risulta necessario "scomodare" le tecniche di cooperazione internazionale dal momento che l'indagine deve essere qualificata come interna e non gestita dallo Stato straniero.

In altri termini, l'intercettazione di comunicazioni che – pur avendo ad oggetto un'utenza straniera o pur essendo compiuta all'estero – sia svolta mediante la tecnica dell'instradamento, non rende necessario il ricorso alla rogatoria poiché l'attività di captazione e registrazione si svolge interamente sul territorio nazionale.

Quello che rileva ai fini della previsione delle forme di assistenza giudiziaria non è il luogo di captazione ma di acquisizione dei risultati appresi mediante intercettazione: così, se gli elementi di prova si trovano all'estero ma, grazie alla tecnologia, diventa possibile apprenderli in Italia, l'indagine deve essere qualificata come "interna".

Nonostante la perimetrazione dell'istituto – almeno nella sua veste tradizionale – abbia trovato una sedimentazione pressoché stabile in dottrina e in giurisprudenza, la questione non è di facile soluzione allorquando, nell'esperimento di investigazioni transfrontaliere, gli inquirenti si avvalgono di nuovi strumenti tecnici di indagine.

In questi casi, non è affatto agevole individuare il *discrimen* tra rogatoria e instradamento: trattandosi di mezzi tecnici itineranti, si pongono difficoltà interpretative sia con riferimento alla verifica della necessità del ricorso alle forme di cooperazione internazionale, sia con riguardo alla tipologia di assistenza da richiedere[64].

[63] Sul tema, diffusamente, S. Allegrezza-F. Nicolicchia, *L'acquisizione della prova all'estero e i profili transnazionali*, in G. Canzio-L.D. Cerqua-L. Luparia (a cura di), *Diritto penale delle società*, Padova, 2014, 1275 ss.

[64] Come affermato dalla giurisprudenza, la rogatoria rappresenta lo strumento ordinario, ma non certo esclusivo, per assumere prove penali o svolgere attività

Tale criticità sembra essere stata superata di recente dalla giurisprudenza di legittimità che, duplicando gli orientamenti già sedimentati in rapporto alle tradizionali intercettazioni itineranti espletate mediante cimici "fisiche"[65] e al meccanismo di captazione dei messaggi del tipo *Blackberry*[66], precisa che «[L']intercettazione ambientale [a mezzo *virus* informatico] installato in Italia su telefono collegato ad un gestore nazionale, non richiede l'attivazione di una rogatoria internazionale per il solo fatto che le conversazioni siano eseguite in parte all'estero, e temporaneamente registrate tramite *wifi* locale, [...] atteso che la captazione ha avuto origine e si è comunque realizzata in Italia, attraverso le centrali di ricezione presso la procura della Repubblica»[67].

La ragione di una simile impostazione deriva, secondo la Corte, non solo dalla presa di coscienza della lentezza della procedura rogatoriale che, evidentemente, mal si concilia con la celerità delle indagini informatiche, ma anche dalla tecnologia propria del *malware*, ossia dalle tecniche di funzionamento e di gestione del materiale raccolto tramite il *virus* informatico.

In effetti, la registrazione dei dati all'estero tramite captatore rappresenta solamente un segmento di una più imponente attività di investigazione che, di fatto, si svolge interamente sul territorio dello Stato: l'ascolto delle conversazioni registrate – che costituisce la fase conclusiva del più complesso *iter* esecutivo delle intercettazioni – viene effettuata in Italia presso gli uffici della procura della Repubblica[68].

investigative all'estero. In questo senso Cass., sez. I, 19 febbraio 1979, n. 8435, in *Cass. pen. mass. annot.*, 1981, 605 ss.

[65] In effetti, la Suprema Corte ha chiarito che «[L']intercettazione di comunicazioni tra presenti eseguita a bordo di una autovettura attraverso una microspia installata nel territorio nazionale, dove si svolge altresì l'attività di captazione, non richiede l'attivazione di una rogatoria per il solo fatto che il suddetto veicolo si sposti anche in territorio straniero ed *ivi* si svolgano alcune delle conversazioni intercettate». In questo senso Cass., sez. III, 19 gennaio 2017, n. 24305, in *C.E.D. Cass.*, n. 269984; Id., sez. II, 4 novembre 2016, n. 51034, *ivi*, n. 268514. Contraria a questa impostazione è la dottrina maggioritaria. Cfr., per tutti, C. Fanuele, *La localizzazione satellitare nelle investigazioni penali*, Milano, 2019, 70 s.

[66] Come rilevato, «[...] l'acquisizione della messaggistica, scambiata mediante sistema *Blackberry*, non necessita di rogatoria internazionale quando le comunicazioni siano avvenute in Italia, a nulla rilevando che per "decriptare" i dati identificativi associati ai codici PIN sia necessario ricorrere alla collaborazione del produttore del sistema operativo avente sede all'estero». Così Cass., sez. IV, 15 ottobre 2019, n. 49896, in *C.E.D. Cass.*, n. 277949. Cfr. anche Id., sez. IV, 8 aprile 2016, n. 16670, *ivi*, n. 266983: Id., sez. III, 29 gennaio 2016, n. 10788, in *Arch. pen.*, 2016, f. 2, 1, Id., sez. VI, 12 dicembre 2014, n. 7634, in *C.E.D. Cass.*, n. 262495.

[67] Così Cass., sez. II, 22 luglio 2020, n. 29362, in *C.E.D. Cass.*, n. 279815.

[68] Più precisamente, nel caso delle attività a mezzo di captatore informatico, la fase prodromica consiste nell'inoculazione all'interno del dispositivo portatile del captatore medesimo e nell'allestimento di tutte le apparecchiature *software* ed *hardware* per consentire l'acquisizione e la ricezione, presso il c.d. punto di consegna allestito nei locali della procura della Repubblica, dei contenuti relativi all'attività di intercettazione dal dispositivo portatile. Tutte queste attività sono svolte dalla polizia giudiziaria sul suolo italiano, con l'ausilio di privati fornitori di servizi aventi sede in Italia.

DPCE online
ISSN: 2037-6677

Conseguentemente, sostengono i giudici, non risulta necessario attivare la procedura prevista e disciplinata dagli artt. 727 ss. c.p.p., poiché il *malware* viene installato nel corso di un'indagine condotta sul territorio dello Stato e la successiva attività di ascolto si svolge interamente sullo stesso.

In questi casi, non sussistendo alcun esercizio della sovranità estera (e ciò anche nel caso in cui parte delle conversazioni sia avvenuta fuori dal territorio in cui l'indagine ha avuto origine), basta ricorrere alla tecnica dell'instradamento.

Poche (e confuse) indicazioni per una sentenza da considerare come una "pioniera" in materia di intercettazioni transnazionali tramite captatore informatico; e, come sempre accade quando ci si confronta con i differenti impieghi del *virus* informatico, la soluzione all'enigma presentato al vaglio di legittimità non risulta pienamente convincente.

Senza voler in questa sede riprendere considerazioni già ampiamente svolte dalla dottrina sul punto[69], basterà dire che le caratteristiche ontologiche del *malware* non permettono di ricorrere così semplicemente alla tecnica dell'instradamento per giustificare il mancato avvio di una rogatoria internazionale. La tecnologia sfruttata in questo caso, infatti, non prevede la creazione di nessun apposito "nodo" telefonico sul territorio italiano: la rete Internet è, per definizione, composta da una moltitudine di nodi. In questo caso, i dati raccolti a mezzo *Trojan* vengono trasmessi – per il tramite del dispositivo "infetto" – al *server* in cui dovranno essere memorizzati. A nulla rileva il fatto che quel *server* sia collocato in Italia: all'atto della registrazione la violazione del diritto a conversare segretamente e riservatamente è già stato violato dal captatore in terra straniera, e la sovranità di quello Stato è già stata violata.

Date le criticità emergenti, una pronuncia di questo genere rappresenta un "precedente" pericoloso nel panorama giurisprudenziale nazionale: legittimando l'impiego processuale dei risultati probatori acquisiti mediante il captatore informatico indipendentemente dal luogo in cui si trovi il soggetto, di fatto la Corte legalizza anche forme di sorveglianza *ultra fines*, peraltro prive di qualsivoglia forma di controllo.

Non solo. Perché così statuendo, i giudici confermano anche la possibilità di procedere all'intercettazione telematica di flussi di comunicazioni allocati su *server* esteri (quali, ad esempio, i dati dinamici contenuti in una casella di posta elettronica o sul *Cloud*), senza necessità di una rogatoria internazionale tutte le volte in cui lo strumento di raccolta delle prove così acquisite è gestito sul territorio italiano.

Di qui, «[S]e già a mezzo dell'istradamento si realizza una captazione *omnibus* di tutte le conversazioni o comunicazioni raccolte per rimbalzo nel fascio instradato dall'ufficio competente nel nostro Paese, il pericoloso connubio con l'uso del captatore occulto, proteso verso utenze o ambienti

[69] P. Maggio, *Intercettazioni* no limits, cit., 459. Cfr., volendo, W. Nocerino, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Cedam, 2021, 360 ss.

sottoposti alla sovranità di Stati esteri, alimenta il presagio funesto di una moltiplicazione – elevata a potenza – di "abusi del processo"»[70].

9. Segue: le acquisizioni negli Stati europei

Una volta individuata la forma di cooperazione cui ricorrere nel caso di intercettazioni all'estero, l'analisi si concentra sulla ricerca dello strumento di assistenza giudiziaria più idoneo allorquando le captazioni a mezzo *Trojan* avvengono tra gli Stati membri dell'Unione europea.

Come noto, l'indiscusso punto di riferimento delle investigazioni unionali è rappresentato dall'Ordine Europeo di Indagine (OEI) che, oramai da qualche tempo, travolge le forme di cooperazione tradizionali allorquando l'indagine è relegata nei confini dell'Unione Europea.

L'obiettivo della sua istituzione è quello di favorire il «*roaming* probatorio»[71] tra i Paesi membri e di recuperare il criterio di radicamento della giurisdizione dello Stato nel quale si trova la persona intercettata o il dispositivo captato.

Più precisamente, l'OEI rappresenta una decisione che viene emessa o convalidata dall'autorità giudiziaria – anche il p.m. o, più in generale, la procura[72] – di un paese dell'UE (c.d. Stato di emissione) per effettuare uno o più atti di indagine in un altro Paese dell'UE (c.d. Stato di esecuzione), al fine di raccogliere elementi di prova in materia penale[73].

Prima facie, può dirsi che l'OEI rattoppa e ricostituisce le falle lasciate dai suoi predecessori: in questo senso, non solo fornisce adeguata risposta alle lungaggini e all'inesauribile burocrazia che caratterizza gli altri strumenti di cooperazione ma soprattutto si distingue per la completezza della sua disciplina, introducendo specifiche norme in rapporto ai differenti atti di indagine[74], di natura atipica.

---

[70] Così P. Maggio, *Intercettazioni* no limits, cit., 463.

[71] L'espressione appartiene a L. Marafioti, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, in T. Bene (a cura di), *L'ordine europeo di indagine. Criticità e prospettive*, Torino, 2017, 11.

[72] Cfr. CGUE, 8 dicembre 2020, n. C-584/19, *Staatsanwaltschaft Wien/A. e.a*, in *Dir. e giust.*, 12 dicembre 2020.

[73] Come anticipato, la direttiva relativa all'Ordine Europeo di Indagine penale è stata adottata il 3 aprile 2014. Sulla direttiva 2014/41/UE, per tutti, T. Bene-L. Luparia-L. Marafioti (a cura di), *L'ordine europeo di indagine. Criticità e prospettive*, Torino, 2016. L'Italia ha provveduto al recepimento della direttiva con il d.lgs. 21 giugno 2017, n. 108, cit. Sul tema, per tutti, F. Ruggieri, *Le nuove frontiere dell'assistenza penale internazionale: l'ordine europeo di indagine penale*, in *Proc. pen. giust.*, 2018, 12 ss.

[74] Quali, ad esempio, le videoconferenze (artt. 18, 19 e 39, d.lgs. 108/2017), le indagini bancarie (artt. 20 e 40, d.lgs. 108/2017), le operazioni sotto copertura (artt. 21-22 e 41 e 42, d.lgs. 108/2017). Inoltre, con riferimento alle intercettazioni, rileva l'estensione della disciplina *ivi* contenuta alla raccolta di dati relativi al traffico telefonico o telematico, nonché l'ubicazione dei dispositivi impiegati (Considerando n. 30 della direttiva). D'altra parte, la possibilità di disciplinare non solo le forme di acquisizione degli elementi di prova, quanto il compimento di tutti gli atti di indagini finalizzati a tale apprensione, costituisce un elemento di valutazione positiva della direttiva,

DPCE online
ISSN: 2037-6677

L'àmbito di applicazione dell'istituto può comprendere, sia nella fase "passiva" che "attiva", tutti gli atti di indagine e di ricerca della prova espressamente indicati dalla direttiva 2014/41/UE: sicuramente di precipuo interesse, quanto alle indagini relative al *cybercrime*, sono le richieste di dati del traffico telefonico e/o di intercettazioni di comunicazioni e le operazioni sotto copertura.

Per quanto attiene alle attività investigative tipiche volte alla captazione di conversazioni e comunicazioni, con l'istituzione dell'OEI viene regolamentata la procedura esecutiva delle intercettazioni transfrontaliere, anche se effettuate per via telematica, da esperire allorquando il dispositivo (o il sistema) da controllare si trovi in uno Stato membro.

In effetti, sia la direttiva 2014/41/UE[75] che il d.lgs. 108/2017[76] dedicano particolare attenzione all'istituto in esame, riferendosi, in modo particolare, alle «intercettazioni di telecomunicazioni», qui da intendersi come captazioni di conversazioni o flussi comunicativi che si avvalgono dell'ausilio di strumenti tecnici, quale il telefono o il *computer*.

Eppure, nonostante la regolamentazione dell'istituto, subentrano delle difficoltà oggettive di adattamento della procedura descritta nel caso delle intercettazioni di comunicazioni tra presenti (art. 266, comma 2, c.p.p.), dal momento che non è chiaro se la disposizione – così come esplicitata dal legislatore europeo e recepita da quello nazionale – possa riferirsi anche a tali forme captative.

Più precisamente, alcuni Autori[77] rilevano che la nuova disciplina relativa all'OEI non sia applicabile alle intercettazioni ambientali che avvengono all'estero, sul presupposto che le formule utilizzate – ossia «indirizzo di comunicazione» (nella direttiva) e «dispositivo o sistema» (nell'atto di recepimento) – non risultano idonee a ricomprendere tali forme di ascolto, dovendosi in questa circostanza far ricorso alla rogatoria internazionale.

Non potendo colmare la lacuna normativa per via interpretativa, si ritiene di dover aderire alla suddetta impostazione e ciò non senza ripercussioni in rapporto ai limiti di impiego del captatore informatico nelle indagini transfrontaliere.

A ben riflettere, dall'assenza di riferimenti espliciti alle intercettazioni

superando i limiti della Decisione Quadro 2008/978/GAI, il cui art. 4, § 2 ne escludeva l'operatività in rapporto alle indagini compiute in tempo reale. In questo senso S. Allegrezza, *Collecting Criminal Evidence Across the European Union: the European Investigation Order Between Flexibility and Proporzionality*, in F. Ruggieri (a cura di), *Transnational Evidence and Multicultural Inquires in Europe. Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Berlino, 2014, 53 s.

[75] La direttiva affronta il tema delle intercettazioni sia nei Considerando nn. 30-31, che, soprattutto nel Capo V, negli artt. 30 e 31, rubricato "*Intercettazioni di telecomunicazioni*".

[76] Più precisamente, agli artt. 23-25 sono dedica le regole inerenti alla procedura passiva, mentre agli artt. 43-45, quelle per la procedura attiva.

[77] C. Parodi, *Il modello C: vecchie criticità e nuovi problemi in caso di intercettazioni all'estero*, in *Dir. pen. cont.*, 1 marzo 2019; F. Siracusano, *La prova informatica transnazionale*, cit., 182 s.

ambientali nel *dictum* legislativo, sembra potersi ricavare un sillogismo perfetto. Se le intercettazioni di comunicazioni e conversazioni tra presenti sono escluse dal perimetro di applicazione dell'OEI e se l'unica attività lecitamente esperibile a mezzo *Trojan* (secondo la legislazione nazionale) è proprio l'intercettazione ambientale, allora se ne deve dedurre che le captazioni da remoto tramite *virus* informatico esulano dalla disciplina dello strumento di cooperazione *intra* unitario.

D'altro canto, non è solo il vuoto di tutela nell'àmbito dell'OEI (e nelle altre norme di cooperazione europea) a preoccupare lo studioso, dovendosi riscontrare la carenza di disciplina delle intercettazioni itineranti transfrontaliere anche in rapporto a tutte le altre forme di cooperazione internazionale. Perché, se è vero – come sostiene la dottrina – che nei casi di intercettazione ambientale euro-unitaria si deve far ricorso all'istituto della rogatoria in assenza di riferimenti normativi espliciti nell'àmbito della direttiva 2014/41/UE e del d.lgs. 108/2017, è altrettanto indiscutibile che l'esecuzione delle operazioni captative a mezzo di *virus* informatico non sono sottoposte nemmeno alle regole in materie di cooperazione internazionale. Come anticipato, infatti, la giurisprudenza più recente[78] ritiene che, allorquando la captazione sia effettuata in un territorio straniero ma l'acquisizione degli elementi probatori avvenga in Italia, non si può ricorrere alla rogatoria, dovendosi far riferimento alla tecnica dell'instradamento.

Di qui, anche il ricorso alla rogatoria (e alle altre forme di cooperazione internazionale) deve ritenersi bandito.

In altri termini, a prescindere dalla tesi da considerarsi prevalente in rapporto alla ricomprensione nel *dictum* dell'OEI delle intercettazioni ambientali, in ogni caso si riscontra un vuoto di tutela che non può ritenersi colmabile in sede applicativa.

Conseguentemente, la mancata armonizzazione a livello europeo della disciplina inerente alle intercettazioni transfrontaliere esperite mediante tecniche di *remote forensics* sottende il rischio di demandare ai giudici il potere discrezionale di scegliere quale normativa applicare nel caso concreto, affidandosi ad una disomogenea giurisprudenza creativa, fatalmente destinata a trasmodare in nomogenesi[79]. E si converrà che è assai discutibile la scelta di affidare alla prassi creativa la disponibilità del ricorso ad uno strumento introdotto con lo scopo di armonizzare le legislazioni internazionali al fine di colmare *deficit* normativi tra gli Stati.

10. L'inutilizzabilità dei dati transfrontalieri

Dall'esegesi delle differenti *species* di investigazioni transnazionali esperibili mediante il ricorso a strumenti tecnici di indagine basati per lo più sui sistemi

[78] Cfr. Cass., sez. II, 22 luglio 2020, n. 29362, cit.
[79] In questo senso, R. Del Coco, *Ordine europeo di indagine e poteri sanzionatori del giudice*, in *Dir. pen. cont.*, 27 dicembre 2015.

DPCE online
ISSN: 2037-6677

di *remote forensics*, emergono evidenti problematiche derivanti dall'assetto predisposto in materia di cooperazione giudiziaria. Nella gran parte delle ipotesi, infatti, l'autorità procedente rimane libera di monitorare conversazioni, flussi telematici e di "gestire" e "controllare" la vita digitale del soggetto "attenzionato" anche al di fuori della propria area di sovranità, prescindendo dalle limitazioni imposte dal sistema legale in cui è localizzato il bersaglio dell'indagine. Sul versante della tutela dei diritti, poi, i destinatari della misura investigativa risultano esposti all'applicazione di un livello di garanzie potenzialmente deteriore rispetto a quello assicurato dal rispettivo ordinamento di appartenenza.

Nonostante la tecnica investigativa produca delle acquisizioni probatorie gravemente lesive di tutti i presidi codicistici, costituzionali e convenzionali, a livello applicativo prevale la linea del massimo uso degli esiti di questo tipo di captazioni, in deroga ai meccanismi propri della cooperazione internazionale.

In questi casi, la tendenza sembra quella di preferire l'àlea dell'incertezza alla categoricità dei moniti normativi: così «lo Stato, anziché attivare gli itinerari "virtuosi" dell'assistenza giudiziaria, [verrebbe autorizzato a forzare] il perimetro di operatività fisiologica della procedura nazionale portando avanti indagini anche oltre i limiti segnati dai confini territoriali, fin quando ciò sia tecnicamente possibile»[80].

Di conseguenza, il discorso non può che incanalarsi sui risultati degli elementi di prova raccolti, sulle eventuali patologie che possono colpirli, fino a travolgere il loro stesso impiego processuale[81].

Sotto un primo aspetto, si potrebbe far rientrare le captazioni itineranti *ultra moenia* tra le attività compiute al di fuori «dei limiti di tempo e di luogo indicati nel decreto autorizzativo», affette – secondo il *dictum* di cui al comma 1-*bis* dell'art. 271 c.p.p. – da inutilizzabilità di tipo patologico. Ma deve accettarsi il rischio che la previsione si risolva in una mera *fictio* priva di effetti invalidanti concreti, essendo assai difficile esplicitare, secondo un «verosimile progetto investigativo»[82], il dettaglio (anche in forma indiretta) dei luoghi in cui si sposterà il dispositivo mobile controllato ovvero la mappatura dei vari soggetti coinvolti.

Posto che la patologia dell'atto di indagine transnazionale non può trovare (solo) la sua fonte nelle regole nazionali che disciplinano l'inutilizzabilità delle intercettazioni *ultra vis*, l'indagine deve concentrarsi sui principi ordinamentali generali che rischiano di essere compromessi

[80] Così F. Siracusano, *La prova informatica transnazionale*, cit., 183.
[81] Con specifico riferimento alla questione dell'utilizzabilità processuale delle prove raccolte all'estero R. Belfiore, *La prova penale raccolta all'estero*, Aracne, 2014, 115 ss.; M. Caianiello, *To Sanction (or not to Sanction) Procedural Flaws at EU Level? A Step forward in the Creation of an EU Criminal Process*, in *Eur. Journal Crime, Crim. Law, Crim. Just.*, 2014, 322 ss.; *giudiziaria*, cit., 3 ss.; M. Daniele, *La sfera d'uso delle prove raccolte*, in *L'ordine europeo di indagine penale*, cit., 181 ss.
[82] P. Maggio, *Intercettazioni* no limits, cit., 471.

dall'espletamento delle tecniche di *live forensics*.

In questo contesto, deve evidenziarsi come sia la stessa Carta costituzionale a predisporre solidi argini atti a presidiare la tutela del principio di sovranità.

Più precisamente, nel caso di investigazioni condotte al di fuori del territorio dello Stato, il potere delle autorità nazionali inquirenti incontra i limiti imposti dall'art. 10 Cost., che circoscrive la sovranità non solo in termini spaziali ma più ampiamente mediante il divieto di compiere, fuori dal territorio interno, atti coercitivi volti a limitare le libertà fondamentali, rendendoli possibili soltanto attraverso l'utilizzo di strumenti di cooperazione conformi «alle norme del diritto internazionale generalmente riconosciute»[83].

Da tale assunto, generalmente condiviso, emerge che l'esercizio di un'attività inquirente o giurisdizionale al di fuori dei confini nazionali realizza una grave violazione delle disposizioni di diritto internazionale tutte le volte in cui manchi un presidio codicistico di riferimento.

Posta la frammentarietà normativa che caratterizza le forme di cooperazione internazionale – soprattutto con riguardo alle intercettazioni itineranti tramite tecniche di *live forensics* –, sorgono dubbi circa la compatibilità delle attività in esame rispetto al diritto internazionale, stante l'assenza di una disciplina stabile che circoscriva i casi e i modi "d'uso".

Un ulteriore limite d'impiego dei risultati investigativi ottenuti mediante l'ausilio di strumenti tecnologici in grado di seguire gli spostamenti del soggetto anche oltre i confini del territorio dello Stato di appartenenza, deriva dalla necessità di garantire il rispetto di quel complesso di norme che tutelano i diritti individuali inevitabilmente compressi dall'espletamento di indagini tecniche.

Più precisamente, al fine di garantire la protezione di tali prerogative, il legislatore (sia a livello interno che internazionale) sembra aver accolto l'auspicio, formulato da una parte degli studiosi[84], della previsione di clausole esplicite di salvaguardia dei diritti fondamentali dei soggetti coinvolti anche – e soprattutto – nel caso di investigazioni transfrontaliere.

Per quanto concerne l'istituto della rogatoria, dal combinato disposto degli artt. 27 e 31 delle preleggi, 191 e 729 c.p.p., si ricava che in ogni caso la prova – anche se raccolta all'estero – non può essere acquisita in contrasto con i principi fondamentali e inderogabili dell'ordinamento giuridico interno.

Una simile impostazione sembra essere suffragata anche dalla giurisprudenza interna, per cui, pur trovando applicazione le norme

[83] In questi termini E. Aprile, *Legittimità delle intercettazioni di telefonate dirette all'estero*, in *Cass. pen.*, 2006, 1837.

[84] Cfr. C. Heard-D. Mansell, *The European Investigation Order: Changing the Face of Evidence-gathering in EU Cross-Border Cases*, in *2 New Journ. Eur. Crim. Law.*, 2011, 365; A. Mangiaracina, *A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order*, in *10 Utrecht L. Rev.*, 2014, 130 s.

processuali dello Stato in cui l'atto viene compiuto, l'unico limite alla validità degli elementi probatori raccolti mediante rogatoria internazionale è che la prova non può essere acquisita in contrasto con i principi fondamentali dell'ordinamento giuridico italiano[85]. Come anche sostenuto, «[È] principio generale in materia di assistenza giudiziaria penale che l'atto compiuto all'estero su rogatoria sia regolato non dalla legge del Paese richiedente, ma, costituendo esso tipico esercizio della sovranità del Paese richiesto, dalle norme dell'ordinamento di quest'ultimo, alla cui stregua deve esserne verificata la validità»[86].

Considerazioni non dissimili valgono in rapporto alle acquisizioni probatorie *intra* europee, per cui il parametro di riferimento è rappresentato – oltre che dai principi interni – anche dal rispetto dei precetti convenzionali.

In questo senso, l'obiettivo è quello di garantire un equo compromesso tra le esigenze investigative e la tutela dei diritti inviolabili così come riconosciuti nell'art. 6 TUE, quali – solo per citare alcuni esempi – il diritto alla dignità umana, alla tutela della libertà personale, alla presunzione di innocenza, alla riservatezza e alla protezione dei dati personali, alla tutela del domicilio e della proprietà[87].

Per quanto concerne l'OEI, il sistema è informato al rispetto del principio di legalità della prova: sia l'art. 1, § 4 della direttiva 2014/41/UE che l'art. 1 del d.lgs. 108/2017 sanciscono il dovere di rispettare i principi dell'ordinamento costituzionale e della Carta dei diritti fondamentali dell'Unione Europea.

Inoltre, pur rimettendo alle scelte dei singoli Stati la valutazione probatoria degli elementi investigativi raccolti all'estero[88], nell'articolato

[85] Così Cass., sez. II, 22 dicembre 2016, n. 2173, in *C.E.D. Cass.*, n. 269000. Nello stesso senso, *ex multis*, Id., sez. VI, 1 dicembre 2010, n. 44488, *ivi*, n. 248963; Id., sez. I, 7 ottobre 2005, n. 45103, *ivi*, n. 232701.

[86] Cass., sez. VI, 19 novembre 1993, n. 2686, in *C.E.D. Cass.*, n. 198237.

[87] Invero, tali prescrizioni potrebbero suonare come «pleonastiche», dato che l'obbligo di rispettare i diritti fondamentali, infatti, è già statuito in modo chiaro dai Trattati (artt. 6 e 21.1 TUE, nonché 67.1 TFUE) e prescritto nella Carta dei diritti dell'UE (V. Titolo I della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), rubricato "Diritti e Libertà". Così R.E. Kostoris, *Ordine di investigazione europeo e tutela dei diritti fondamentali*, in *Cass. pen.*, 2018, 1438. Inoltre, è ribadito costantemente dalla Corte di giustizia (*ex multis*, CGUE, 26 febbraio 2013, *Åklagaren c. Åkerberg Fransson*, C-617/10, § 45 s., secondo cui i giudici nazionali hanno il potere di "valutare pienamente", se del caso con la "collaborazione" della Corte di giustizia, la compatibilità del diritto interno attuativo del diritto dell'Unione con le prescrizioni della Carta di Nizza) e dalla Corte EDU. Solo per citare alcune pronunce più recenti in rapporto all'esperimento di atti investigativi lesivi delle prerogative individuali, Corte EDU, sez. V, 17 dicembre 2020, *Saber c. Norvegia*, n. 459/18; Id., sez. II, 8 dicembre 2020, *Bostan c. Moldavia*, n. 52507/09; Id., sez. IV, 14 aprile 2020, *Dragan Petrovic c. Serbia*, n. 75229/10; Id., sez. III, 4 febbraio 2020, *Kruglov c. Russia*, n. 11264/04; Id., sez. V, 30 gennaio 2020, *Vinks and Ribicka c. Lettonia*, n. 28926/10.

[88] Ai sensi dell'art. 14, § 7, «[…]. Fatte salve le norme procedurali nazionali, gli Stati membri assicurano che nei procedimenti penali nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite tramite l'OEI».

legislativo sono previste – più o meno esplicitamente – regole di esclusione delle prove acquisite *contra legem*. Solo a titolo esplicativo, si pensi all'art. 6, § 1 della direttiva, trasposto nell'art. 27 del decreto in rapporto all'inutilizzabilità delle prove acquisite in violazione dei requisiti nazionali di ammissibilità; all'art. 9, § 2 della direttiva, trasfuso nell'art. 4, commi 2, 3 e 5 del decreto in rapporto alle prove acquisite violando le norme sul *quomodo* delle attività istruttorie; l'art. 36 del decreto in rapporto all'inutilizzabilità per l'inosservanza delle garanzie difensive.

Pur prescrivendo tali regole processuali, la direttiva tace completamente in merito ad eventuali conseguenze derivanti dalla loro violazione: il par. 1 dell'art. 14, infatti, si limita ad affermare che gli Stati membri «shall ensure that legal remedies equivalent to those available in a similar domestic case, are applicable to the investigative measures indicated in the EIO». Molto semplicemente, pertanto, tramite una clausola di equivalenza, viene fatto rinvio gli strumenti di doglianza già predisposti nel diritto interno in relazione alle medesime attività istruttorie.

Senza entrare nel merito dei rimedi esperibili contro le violazioni dei diritti fondamentali, dall'esegesi delle norme che tipizzano le *exclusionary rules* si ricava un principio generale di diritto consistente nell'impossibilità di procedere ad investigazioni transfrontaliere per l'acquisizione di elementi probatori utili alle indagini disattendendo le regole di ammissibilità delle prove operanti a livello nazionale, pena l'inutilizzabilità delle informazioni raccolte.

In altre parole, allo stato attuale, spetta al solo diritto nazionale stabilire le regole relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti criminali, di informazioni e di elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati, contraria al diritto dell'Unione (c.d. principio di autonomia procedurale).

Come noto, tali regole impongono che, perché un atto investigativo possa limitare le prerogative fondamentali, l'ingerenza deve essere espressamente prevista dalla legge e deve sussistere un provvedimento giurisdizionale sufficientemente motivato atto a legittimare la compressione.

In base alla ricostruzione offerta, devono ritenersi vietate le investigazioni digitali a distanza di tipo dinamico, essendo finalizzate alla sorveglianza continuativa di dispositivi informatici (anche situati all'estero) e al monitoraggio delle attività in Rete compiute attraverso i medesimi in assenza di una copertura normativa stabile e onnicomprensiva e di un'esplicita autorizzazione giurisdizionale all'esecuzione delle operazioni *de quibus*.

Di qui, i risultati investigativi acquisiti in Paesi diversi da quello in cui è avviata l'indagine devono ritenersi inutilizzabili perché contrari alle regole probatorie sedimentate nell'ordinamento nazionale.

Si potrebbe, a questo punto, parlare di una proiezione dell'inutiliz-

DPCE online
ISSN: 2037-6677

zabilità interna a livello internazionale per quegli atti probatori che – già sul versante interno – sono affetti da inutilizzabilità per incostituzionalità.

Ma se questa può essere la soluzione alle funzioni atipiche del *virus* informatico che, è bene ribadirlo, non trovano alcun riferimento normativo esplicito né a livello nazionale né in quello sovranazionale, *quid iuris* per l'attività intercettiva *stricto sensu* intesa?

In generale, può dirsi che solo in poche e oramai risalenti occasioni l'inutilizzabilità degli atti ha trovato riconoscimento a fronte di utenze intercettate senza ricorrere alle pratiche giudiziarie e amministrative sancite ed imposte dalle Convenzioni internazionali[89].

La *quaestio* è destinata a complicarsi ulteriormente nel caso di intercettazioni ambientali transfrontaliere, per cui la disciplina vigente – scarna ed evanescente, quasi insistente – sembra lasciare ampi spazi di manovra per bypassare le regole della cooperazione internazionale.

Come ormai noto, l'OEI non fornisce adeguata disciplina alle intercettazioni di conversazioni e di comunicazioni tra presenti transfrontaliere e, colmando per via interpretativa il vuoto normativo, la giurisprudenza ricorre all'istituto dell'instradamento per giustificare le captazioni all'estero.

In questi casi, dunque, non si applicano le regole esistenti in materia di cooperazione giudiziaria, dovendosi ritenere valida e legittima la disciplina nazionale.

Tuttavia, anche la scelta di estendere alle intercettazioni ambientali itineranti condotte – parzialmente – all'estero la normativa prevista dall'ordinamento interno, non sembra persuasiva, risultando altamente pericolosa per la tutela delle prerogative inviolabili.

A ben riflettere, una simile impostazione genera non pochi punti di frizione con il *dictum* di cui all'art. 8 CEDU che, ai fini della legittimità delle intercettazioni, non richiede solo la sussistenza di una base legale ma anche la sua accessibilità e prevedibilità per il soggetto sottoposto alla misura[90].

E proprio quest'ultimo requisito non può ritenersi soddisfatto seguendo l'orientamento richiamato.

Come rilevato dalla più attenta dottrina, «[…] nel momento in cui un

[89] Cfr. Tribunale di Roma, 20 ottobre 2000, in *Giust. pen.*, 2001, 120; tribunale di Bologna, 23 giugno 1998, in *Cass. pen.*, 2000, 1058.

[90] Corte EDU, Grande Camera, 16 febbraio 2000, *Amann c. Svizzera*, n. 27798/95; Id., Grande Camera, 24 aprile 1990, *Kopp c. Svizzera*, n. 23224/94, § 64; Id., Grande Camera, 2 agosto 1984, *Malone c. Regno Unito*, cit., § 66; Id., Grande Camera, 26 aprile 1979, *Sunday Times c. Regno Unito*, n. 6538/74, § 49. Più di recente, Id., sez. III, 17 ottobre 2017, *Navalnyye c. Russia*, n. 101/15; Id., sez. IV, 14 aprile 2015, *Contrada c. Italia*, n. 66655/13, §§ 60–63. Per dovere di completezza, preme sottolineare che la Corte in altra occasione ha chiarito che non sussiste alcuna incompatibilità tra la procedura di instradamento e l'art. 8 CEDU, dal momento che, pur se non espressamente prevista dalla legge, risulta legittimata da giurisprudenza consolidata e, inoltre, è da considerarsi necessaria in una società democratica perché funzionale all'accertamento di gravi reati. Così Id., sez. I, 23 febbraio 2016, *Capriotti c. Italia*, 28819/12, § 44.

soggetto si trova in un territorio estero, è ragionevole pensare che, a prescindere dalla sua nazionalità, nutra l'aspettativa che un'eventuale intercettazione avvenga secondo la legislazione processuale che vige in quel Paese [...]. Diversamente, si dovrebbe ritenere che le comunicazioni possano essere oggetto di captazione da parte di qualunque Stato che sia tecnicamente in grado di intercettarle e che magari effettui la captazione con garanzie inferiori a quelle attribuite dal Paese in cui si trova»[91].

Wanda Nocerino
Dip.to di Giurisprudenza
Università degli Studi di Foggia
wanda.nocerino@unifg.it

[91] In questi termini S. Signorato, *Le indagini digitali*, cit., 165, la quale con riferimento alla più generale tecnica di instradamento, rileva come la stessa «sembra pure aggirare l'art. 31.1 della direttiva 2014/41/UE, relativa all'OEI, laddove prevede che anche quando non sia necessaria l'assistenza tecnica di un altro Stato, ma l'indirizzo di comunicazione della persona sottoposta ad intercettazione venga impiegato sul territorio di un altro Stato, lo Stato membro di intercettazione deve dare notifica allo Stato su cui viene utilizzato l'indirizzo di comunicazione dell'intercettazione stessa».