DIPARTIMENTO DI GIURISPRUDENZA
Cattedra di Diritto Processuale Penale

LA RICERCA DELLA PROVA PENALE MEDIANTE *VIRUS* INFORMATICO

RELATORE
Chiar.mo Prof. Paolo Moscarini

CANDIDATA
Valeria Apicella
126953

CORRELATORE
Chiar.ma Prof.ssa Maria Lucia Di Bitonto

Anno accademico 2017/2018

Indice

Premessa 7

CAPITOLO I

Le tecnologie informatiche ed i diritti fondamentali

1. L'impatto della tecnologia sulla ricerca della prova penale 10
2. I "captatori informatici" 14
3. Diritti inviolabili e doveri inderogabili 19

CAPITOLO II

Le intercettazioni mediante l'impiego di un *virus* informatico

1. Le intercettazioni di conversazioni o comunicazioni mediante captatore informatico 25
2. La sentenza *Scurato*: le intercettazioni "peripatetiche" 26
3. Profili critici e possibili soluzioni 29
4. L'inutilizzabilità: una sanzione adeguata? 32
5. La discussa rilevanza del luogo ed i requisiti del decreto di autorizzazione 33
6. Una questione dirimente: la nozione di criminalità organizzata 38
7. La captazione di flussi informatici o telematici 43
8. Le intercettazioni di comunicazioni *Voice over Internet Protocol* (VoIP) 46
9. Il caso *Occhionero*: prime applicazioni pratiche del captatore informatico alle intercettazioni telematiche 50

CAPITOLO III

Le ispezioni e le perquisizioni "a distanza"

1. Cenni introduttivi 53
2. L'ispezione informatica mediante "virus" 56
3. …ed i relativi profili problematici 58
4. (segue). L'esigenza di un livello minimo di garanzie per l'utilizzo del captatore informatico 62
5. La perquisizione *online* 63
6. …e la sua ritenuta ammissibilità 66

7. Il divieto di perquisizioni esplorative.....69
8. L'inammissibilità di perquisizioni occulte.....72

CAPITOLO IV

I sequestri digitali "statici" e "dinamici"

1. Il sequestro informatico.....76
2. …ed i relativi aspetti problematici.....79
3. Il sequestro mediante l'utilizzo di un captatore informatico.....83
4. Circa l'ammissibilità di un sequestro informatico mediante captatore.....85
5. La captazione della posta elettronica e delle *e-mail* in "bozza" mediante *virus* informatico 90
6. L'equiparazione giurisprudenziale delle *e-mail* alla prova documentale……...99

CAPITOLO V

La novella riguardante le intercettazioni e l'impiego di un "captatore informatico"

1. Brevi cenni a margine della riforma in materia di intercettazioni.....103
2. La neo-introdotta disciplina delle intercettazioni tra presenti mediante l'utilizzo di un captatore informatico.....105
3. Le intercettazioni tra presenti "semplificate" in relazione ai delitti contro la P.A.....109

Conclusioni..... 113

Bibliografia..... 116

Riferimenti giurisprudenziali 125

Alla mia famiglia

«I devoti di ogni devozione son tanti e sempre pronti ad accendere il fuoco sotto chi non si conforma alla loro devozione; e gli increduli, coloro che su ogni cosa esercitano facoltà di critica, che nulla accettano se non per vaglio di ragione, son pochi e non tollerati».

L. Sciascia

PREMESSA

Il presente elaborato, senza alcuna pretesa di completezza, si propone di analizzare talune delle questioni connesse all'ingresso della tecnologia nel procedimento penale, con particolare riguardo al caso in cui le "chiavi d'accesso" sono costituite dalle indagini informatiche.

Di queste ultime si parla non solo quando il sistema informatico o telematico costituisce il corpo del reato o una cosa ad esso pertinente (e, quindi, l'*oggetto* dell'indagine); ma, altresì, allorché l'autorità giudiziaria faccia ricorso agli strumenti tecnologici come *mezzo* per condurre una investigazione. Ed è su tale secondo profilo che è incentrato il presente studio.

I dispositivi elettronici, in particolare quelli portatili, costituiscono ormai un'appendice indispensabile della persona. I soggetti coinvolti nella fase investigativa, dagli organi inquirenti all'indagato, non sono altro che una proiezione in scala ridotta di una società informatizzata, in cui la condivisone di abitudini digitali costituisce il minimo comune denominatore.

Così, telefoni cellulari, *computer*, *tablet* diventano il contenitore di elementi probatori digitali, assai rilevanti ai fini dell'accertamento dei fatti, la cui estrazione è resa possibile dai mezzi di ricerca della prova.

Ebbene, la tecnologia rende oggi possibile ricercare e acquisire le informazioni contenute nei suddetti dispositivi elettronici attraverso l'utilizzo di un "captatore informatico"; ovvero, di un programma installato via *hardware* o via *software* nel dispositivo elettronico in uso al soggetto *target*.

Trattasi allora di stabilire se la normativa vigente consenta una tale operazione investigativa.

Quest'ultima, a seconda della funzione attivata, potrebbe via via essere assimilata e quindi ricondotta alle intercettazioni, alle ispezioni, alle perquisizioni ovvero ai sequestri, declinati in chiave dinamica ed occulta. Ma, com'è noto, solo le intercettazioni e la disciplina ad esse relativa sottendono una captazione occulta. Mentre le altre attività di ricerca della prova debbono avere, secondo la normativa vigente, un carattere palese, cosicché è più difficile ricondurre alle stesse un'ispezione, perquisizione o sequestro realizzati, in modo occulto, mediante il "captatore informatico".

Lo sforzo di ricondurre ciascuna fase relativa alla ricerca della prova digitale mediante *virus* all'istituto giuridico *viciniore* non è fine a sé stesso, ma è finalizzato ad assicurare la possibilità legale e l'attendibilità giuridica del risultato, strettamente connessi alla tutela dei diritti fondamentali, la compressione dei quali è di regola soggetta ai principi della riserva di legge e della tassatività.

Al riguardo, le soluzioni che di seguito si tentano di proporre, ove esistenti, non offrono una risposta univoca.

Nei casi in cui, come si vedrà, la sussunzione dell'indagine informatica mediante "captatore" all'interno delle prove tipiche non possa essere ammessa, l'alternativa potrebbe consistere nel ricondurre tale speciale investigazione nell'alveo delle prove atipiche *ex* art. 189 c.p.p.; ma ciò implica comunque un previo vaglio tendente a stabilire la compatibilità costituzionale del mezzo di prova. L'esito positivo del quale non è sempre scontato con riguardo all'utilizzo del captatore informatico.

Quest'ultimo, fungendo da vero e proprio catalizzatore dei mezzi di ricerca della prova, consente un aumento considerevole della velocità di acquisizione delle informazioni digitali che rischia di travolgere le garanzie poste dall'ordinamento a protezione del diritto di difesa e del diritto al contraddittorio, nonché di causare, inevitabilmente, un'alterazione irreversibile del risultato finale.

CAPITOLO I

Le tecnologie informatiche ed i diritti fondamentali

Sommario: 1. L'impatto della tecnologia sulla ricerca della prova penale. - 2. I "captatori informatici". - 3. Diritti inviolabili e doveri inderogabili.

1. L'impatto della tecnologia sulla ricerca della prova penale

L'incontro tra informatica e processo penale, tra scienza e diritto, si riflette in modo assai rilevante sull'attività investigativa e sulla ricerca della prova. I punti di intersezione sono individuabili su vari livelli.

In primo luogo, i mezzi tecnologici possono venire in rilievo come l'oggetto stesso di un'attività di indagine, in quanto depositari di informazioni rilevanti.

La L. 18 marzo 2008, n. 48[1], ha espressamente esteso l'ambito di applicazione dei mezzi di ricerca della prova anche ai sistemi informatici e telematici (cfr. artt. 244, 247, co. 1 *bis*, 254 *bis*, 354 c.p.p.).

In secondo luogo, lo strumento tecnologico può essere impiegato come mezzo alternativo per la raccolta di una prova "tradizionale". Si pensi all'esame a distanza mediante collegamento audiovisivo (art. 147-*bis*, co. 2, norme att. c.p.p.), ovvero ad una ricognizione a distanza[2], utilizzabile come prova atipica *ex* art. 189 c.p.p[3].

---

[1] *"Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno",* pubblicata nella Gazzetta Ufficiale, n. 80, 4 aprile 2008, supplemento ordinario n. 79. Per ulteriori approfondimenti, cfr. M. L. DI BITONTO, *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. Internet*., 2008, p. 503 ss.; L. LUPARIA*, La ratifica della Convenzione cybercrime del Consiglio d'Europa. Legge del 18 marzo del 2008, n. 48. I profili processuali*, in *Dir. pen. proc*., 2008, p. 717 ss.

[2] P. MOSCARINI, *Lineamenti del sistema istruttorio penale*, Torino, 2017, p. 107.

[3] Dopo un primo vano tentativo di introduzione del principio di tassatività in materia di strumenti istruttori con la legge delega del 3 aprile 1974 n. 108, il successivo progetto preliminare, attuativo della legge delega del 16 febbraio 1987, n. 81, conferisce fondamento normativo alle prove cosiddette atipiche nell'art. 189 del codice di rito.

Non dissimilmente, si potrebbe documentare l'attività investigativa o rappresentare fatti, persone o cose attraverso apparecchi di fono e/o videoregistrazione.

Infine, un'ulteriore – ma più problematica – applicazione delle tecnologie informatiche al procedimento penale investe direttamente lo strumento investigativo e il metodo di ricerca della prova, nel senso che la tecnologia informatica è lo strumento attraverso il quale vengono captate e documentate informazioni che sarebbe stato altrimenti impossibile raccogliere.

A tal proposito, vengono in rilievo, senza alcuna pretesa di esaustività, la localizzazione satellitare mediante GPS, l'acquisizione dei dati di ubicazione del telefono cellulare, le intercettazioni di comunicazioni informatiche o telematiche e – con una più marcata coloritura critica – l'installazione di un *software* o *virus* o "captatore" informatico in grado di esplorare e, in alcuni casi, di "fotografare" il contenuto di un dispositivo elettronico (es. un telefono cellulare, un *tablet,* un *personal computer*), seguendone l'attività attraverso una sorta di *shadowing*.

In questo caso, lo strumento informatico è al contempo soggetto e oggetto dell'attività di inchiesta, nonché mezzo di documentazione. Di qui, l'estrema delicatezza di siffatta operazione, che impone un elevato grado di cautele e garanzie, a tutela dei diritti inviolabili della persona e del principio di legalità processuale stabilito dall'art. 111 comma 1 Cost.

Invero, la promiscuità dei dati informatici contenuti, ad es., all'interno di un telefono cellulare oggetto di investigazione non consente di distinguere *ex ante* tra dati strettamente personali e dati rilevanti ai fini dell'accertamento del reato.

Il rischio che i primi vengano comunque intaccati dall'attività d'inchiesta, malgrado la loro estraneità ai fatti oggetto di accertamento, aumenta il pericolo di lesione dei diritti fondamentali, in particolare del diritto alla riservatezza.

Il principio di tassatività resta sullo sfondo, dal momento che il legislatore non fissa un criterio di totale libertà delle prove, ma ancora la legalità del risultato probatorio alla coesistenza di tre requisiti, di cui l'ultimo rappresenta più precisamente una condizione procedurale: 1) idoneità ad assicurare l'accertamento dei fatti; 2) assenza di pregiudizio alla libertà morale della persona; 3) attivazione del contraddittorio tra il giudice e le parti circa le modalità di assunzione della prova.

A tale rischio, si aggiunga l'immanente volatilità dei dati informatici e la possibile alterabilità degli stessi, che impongono che ogni anello della c.d. *chain of custody* veda assicurate la fedeltà all'originale, la corretta conservazione e l'immodificabilità[4]. Infatti, si è autorevolmente osservato che «*il giusto processo deve riconoscere all'imputato il diritto di essere messo a confronto con il dato informatico nel suo aspetto genuino, senza alterazioni*» quale *«trasposizione moderna del diritto a confrontarsi con l'accusatore*»[5].

Ed ancora, si consideri che, con riguardo alle informazioni digitali, il relativo salvataggio, o comunque la conservazione, sono affidati spesso a *servers* o *providers* che non hanno sede in Italia. Di qui l'esigenza di una rogatoria per acquisire tali informazioni, eventualmente rilevanti ai fini procedimentali penali, con conseguente aggravio dei tempi del procedimento.

Tuttavia, se ci si limita alla raccolta di dati quali i c.d. *logs* di accesso (data, ora e indirizzo IP di ogni *log in*, ovvero di ogni connessione ad Internet effettuata tramite un determinato, terminale, ad es. un PC o un telefono cellulare) e a generali informazioni di base (nominativo, numero di telefono, *email* utilizzata per l'iscrizione, eventuale metodo di pagamento), è in genere sufficiente una richiesta da parte dell'autorità giudiziaria rivolta direttamente al *provider*[6].

---

[4] La legge 48/2008 ha previsto, tra l'altro, l'adozione di misure tecniche dirette ad assicurare la conformità dei dati acquisiti all'originale, l'immodificabilità e l'integrità degli stessi. Dall'analisi di alcune delle più comuni *best practices*, caratterizzate da generalità, pubblicità e accettazione da parte della comunità scientifica, emerge un quadro di riferimento comune. In particolare, si richiede che il *Digital evidence first responder* (DEFR), l'operatore che per primo viene a contatto con i dispositivi elettronici contenenti le evidenze probatorie digitali, abbia un'adeguata esperienza e le competenze tecniche necessarie per procedere alla messa in sicurezza e all'isolamento dell'area in cui si svolge il cosiddetto incidente informatico. Il primo passaggio consiste nell'identificazione della fonte di prova. In ogni caso, la gestione dei dati acquisiti dal dispositivo elettronico dovrà rispondere ai seguenti requisiti: a) pertinenza: rilevanza dei dati; b) affidabilità, espressa in termini di genuinità e verificabilità *ex post* dei passaggi compiuti; c) sufficienza: contemperamento tra le esigenze di completezza del quadro probatorio digitale e il principio del minimo mezzo, a cui si ispira l'acquisizione parziale dei dati, laddove possibile; d) giustificabilità: adozione delle migliori tecniche attuabili, tenendo conto delle esigenze tecniche del caso concreto.
A tali fini, risulta di fondamentale importanza la completezza della documentazione, anche fotografica, che dovrà dare conto delle scelte compiute e delle tecniche utilizzate, nonché indicare ogni operazione effettuata, gli eventuali errori commessi, i soggetti coinvolti nell'incidente informatico, lo stato in cui il dispositivo è rinvenuto.

[5] P. TONINI, *Documento informatico e giusto processo*, *in Dir. pen. proc*., 2009, p. 406.

[6] I *providers* più comuni (ad esempio, *Facebook*, *Snapchat*, *Skype*) sono ubicati negli Stati Uniti, dove manca una legge che impone la conservazione dei dati per un certo periodo di tempo. Pertanto, è fondamentale una richiesta di congelamento dati da parte dell'autorità giudiziaria direttamente al *provider* di riferimento, valida generalmente per 90 giorni con possibilità di proroga.
Tuttavia, occorre considerare che *WhatsApp*, ad esempio, non conserva lo storico delle connessioni, né quello relativo alle chiamate o ai messaggi. Per quanto concerne le informazioni di registrazione, il

Qualora, invece, si miri ad ottenere i c.d. "*activity logs*" relativi ai dati telematici (mittente e destinatario, data, ora, durata e "dimensione" della comunicazione), sarà necessario procedere con una richiesta rogatoriale indirizzata all'autorità straniera nella cui giurisdizione il *provider* ha sede. Ma la stessa localizzazione dei dati, necessaria per l'individuazione dell'autorità straniera destinataria della rogatoria, può rivelarsi non decisiva, qualora gli stessi siano salvati in *Internet* servendosi del c.d. *cloud computing*[7]. In tal caso, poiché il gestore può spostare i dati da un *server* all'altro in ogni momento per esigenze tecniche, economiche o organizzative (c.d. *load balancing*)[8], diventa assai complicato individuare il Paese in cui i dati hanno sede e, quindi, l'Autorità giudiziaria alla quale rivolgersi.

In conclusione, se da un lato non è possibile negare le potenzialità applicative e l'utilità gnoseologica delle indagini informatiche (e, in particolare, di quelle condotte attraverso l'utilizzo di un *virus* o "captatore" informatico), dall'altro lato, sussistono rilevanti problematiche e rischi legati alla potenziale erosione dei diritti fondamentali, di fronte al quale né l'interprete, né soprattutto il legislatore possono restare inerti.

A tal proposito, già nel 2001 è stata siglata a Budapest la Convezione del Consiglio d'Europa, volta ad armonizzare le legislazioni nazionali nella lotta comune contro la criminalità informatica.

La Legge 18 marzo 2008, n. 48, con cui è stata ratificata la Convezione, ha ricondotto l'attività di reperimento e di apprensione del dato digitale ai mezzi tipici di ricerca della prova ovvero, a seconda dei casi, agli accertamenti urgenti di polizia giudiziaria. In ogni caso, la peculiarità dell'oggetto su cui ricadono tali atti investigativi, impone l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati digitali e ad impedirne l'alterazione, provvedendo, ove possibile, alla loro immediata duplicazione su supporti idonei, con procedure in grado di garantire la conformità

---

provider può fornire i seguenti dati: 1) numero di telefono; 2) data di registrazione al servizio; 3) *username*, se l'utente utilizza uno *smartphone* di tipo *Blackberry* o *iPhone*; 4) dati relativi all'ultimo utilizzo; 5) stato dell'*account*; 6) dispositivo utilizzato; 7) utenti bloccati dall'utilizzatore e utenti che hanno bloccato il numero dell'utilizzatore, impedendo la ricezione di messaggi da parte del destinatario del blocco.

[7] La memorizzazione e l'elaborazione dei dati avviene attraverso *hardware* e *software* localizzati in *Internet* – si pensi a "*Dropbox*" o "*iCloud*".

[8] Per ulteriori approfondimenti sulla "*relazione pericolosa tra prova informatica e raccolta transfrontaliera*", vedi F. SIRACUSANO*, La prova informatica*, in *Investigazioni e prove transnazionali*, XXX Convegno Nazionale, Associazione tra gli studiosi del processo penale "G. D. Pisapia", Roma 20-21 ottobre 2016, Università La Sapienza, p. 4.

all'originale e l'integrità dei dati copiati. Tale adeguamento normativo all'evoluzione tecnologica ha lasciato, tuttavia, irrisolti taluni problemi applicativi[9].

Pertanto, si è reso necessario un ulteriore intervento normativo: nel nostro Paese, la Legge 23 giugno 2017, n. 103[10], *inter alia*, ha delegato il Governo a riformare il processo penale, con particolare riguardo alla disciplina delle intercettazioni e, in generale, delle operazioni captative (cfr. Cap. V).

Dopo il primo via libera del Consiglio dei Ministri in data 2 novembre 2017, il testo passa all'esame delle Commissioni Giustizia per i relativi pareri. Nel corso della stesura del presente elaborato, la delega è stata attuata con il d.lgs. 29 dicembre 2017, n. 216[11], di cui si discuterà *infra* (cfr. Cap. V).

2. I "captatori informatici"

Tra le indagini informatiche, spiccano per potenzialità investigativa (ma anche per la possibile compressione dei diritti fondamentali) quelle condotte mediante l'utilizzo di captatori informatici. Ovvero di *software* o *virus* informatici in grado di esplorare e, in alcuni casi, di "fotografare" il contenuto di un dispositivo elettronico (es. un telefono cellulare, un *tablet,* un *personal computer*), seguendone l'attività attraverso una sorta di *shadowing*.

L'installazione furtiva del captatore può avvenire sia mediante l'accesso fisico al dispositivo *target* – ipotesi più rara – sia a distanza, mascherandolo nell'allegato di una *email*, nell'aggiornamento di un'applicazione o in una comunicazione inviata da servizi

[9] Sul carattere prevalentemente didascalico della L. 18 marzo 2008, n. 48, si veda F. M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen*., 2012, n. 2, p. 703.

[10] "*Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario*", pubblicata in *Gazzetta Ufficiale* n. 154, 4 luglio 2017. Il punto di partenza dell'*iter* normativo è costituito dalla proposta di legge C. 4260, depositata alla Camera dei Deputati il 31 gennaio 2017. In data 15 marzo 2017, viene approvato in Senato il disegno di legge n. 2067 (*Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario*), convertito nella legge n. 103, 23 giugno 2017.

[11] *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*. G.U. Serie Generale n. 8, 11 gennaio 2018.

di messaggistica. Esso si compone di due moduli: il primo, il *server*, infetta il dispositivo bersaglio; il secondo, il *client*, ne effettua il controllo.

La molteplicità di funzioni che contraddistinguono un captatore informatico lo rendono uno strumento dalle potenzialità applicative ampie, che ne complicano il bilanciamento con i diritti a tutela costituzionale rafforzata e – in assenza di una specifica ed espressa previsione normativa – potrebbero renderne dubbia l'ammissibilità nel nostro ordinamento giuridico.

Le principali funzioni che attualmente il captatore informatico è in grado di svolgere, ma non si esclude un possibile futuro ampliamento e perfezionamento delle stesse, consistono, come anticipato, nella captazione del traffico dati in entrata e in uscita (posta elettronica, navigazione in Internet), delle digitazioni sulla tastiera (*keylogger*) e delle visualizzazioni sullo schermo (*screenshot*), nella memorizzazione del contenuto dell'*hard disk* con possibilità di copiare, in tutto o in parte, le unità di memoria del sistema informatico.

È altresì astrattamente possibile inserire nuovi dati nel dispositivo elettronico sottoposto a controllo o cancellare quelli esistenti, geolocalizzare il dispositivo con un livello di precisione inferiore ai 20 metri[12], nonché attivare da remoto la *webcam* o il microfono[13], così da captare suoni e conversazioni aventi luogo in prossimità del dispositivo.

---

[12] La localizzazione mediante i dati di ubicazione del telefono cellulare può essere semplice o storica, e quindi statica, oppure di precisione (il cosiddetto "*positioning*"), con informazioni aggiornate ad intervalli regolari predefiniti. Nel primo caso, i dati sono già precostituiti e preesistono all'intervento degli organi inquirenti; nel secondo caso, invece, la rilevazione dei dati avviene in tempo reale, realizzando un un'attività di c.d. *online surveillance*. La Corte di Cassazione [Cass., Sez. I, 28 maggio 2008, n. 21366, in *C.E.D. Cass*., n. 240092] ha ricondotto la tecnica del *positioning* ad un'attività da cui trarre tracce e elementi di prova, che «*può farsi rientrare negli atti urgenti demandati agli organi di Polizia Giudiziaria, ai sensi degli artt. 55 e 348 c.p.p. e, come tale, non è subordinata alla preventiva autorizzazione da parte dell'autorità giudiziaria, consistendo l'operazione in una sorta di pedinamento a distanza*». Tuttavia, sarebbe preferibile l'adozione di un decreto autorizzativo del pubblico ministero.
Per ulteriori approfondimenti sul tema, si veda G. DI PAOLO*, Acquisizione dinamica dei dati relativi all'ubicazione del cellulare ed altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, in *Cass. pen.*, n. 3, 2008, p. 1227.

[13] Per ulteriori approfondimenti sulle funzioni del *trojan horse* si veda M. ZONARO, *Il Trojan - Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento di intercettazione*, in *Parole alla difesa*, 2016, n. 1, p. 164.

Tali attività vengono anche definite di "*online search"* e "*online surveillance"*, autorevolmente tradotte rispettivamente come "copiatore informatico" e "appostamento informatico"[14].

La prima permette di entrare nella memoria del sistema informatico interessato e far copia totale o parziale dei dati in essa contenuti. Non a caso, viene anche definita *one time copy*.

Nella seconda categoria, invece, rientrano quei programmi spia aventi ad oggetto il flusso informativo di un sistema informatico o telematico, o intercorrente tra due o più sistemi informatici o telematici, che passa attraverso la rete Internet (ad esempio, *e-mail*, siti visitati, *files* scaricati, *chat*, ora e durata delle connessioni). Secondo taluni autori, rientra nella "sorveglianza online" anche il flusso di dati intercorrente tra le periferiche (microfono, *webcam*, tastiera) ed il microprocessore del dispositivo *target*, che consente il monitoraggio in tempo reale del contenuto delle digitazioni sulla tastiera (*keylogger*), delle visualizzazioni sullo schermo (*screenshot*) e delle comunicazioni via microfono e via *webcam*[15].

Secondo altri, invece, tali tipologie di programmi configurano una sorta di *tertium genus*, con caratteristiche miste, in parte mutuate dall'*online search*, in parte *dall'online surveillance*. L'inquadramento tecnico di tali attività non è un mero esercizio privo di conseguenze pratiche, ma rileva ai fini dell'eventuale inquadramento giuridico, che sarà oggetto di successiva trattazione.

L'unica costante del captatore è individuabile nel suo carattere occulto, poiché agisce indisturbato, sfuggendo agli antivirus in commercio e ai *firewall*. Un segnale d'allarme per il soggetto *target* – semmai – è costituito dal maggiore consumo di batteria, che aumenta in relazione al numero delle funzioni abilitate e alla durata dell'appostamento informatico.

La trasmissione dei dati raccolti ad un altro sistema informatico in uso agli investigatori avviene in tempo reale o ad intervalli predeterminati.

---

[14] M. TROGU, *Sorveglianza e "perquisizione" online su materiale informatico*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, pp. 442 e 445.

[15] P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, *in Processo penale e giustizia*, n. 5, 2016, p. 124.

Sin qui è facile intuire l'impossibilità di sussumere all'interno di un'unica fattispecie le varie attività che il captatore può svolgere, ammesso che una qualche sussunzione sia possibile.

Sul punto manca unanimità di vedute.

Da un lato, taluni sostengono l'inammissibilità di tale strumento intrusivo in assenza di una specifica disciplina normativa che attui il corretto bilanciamento tra i diritti fondamentali dell'individuo e le esigenze investigative.

In tal senso, con riguardo al diverso caso delle videoriprese domiciliari, la Corte Costituzionale ha affermato la non conformità al modello costituzionale di un processo non "giusto" perché carente sotto il profilo delle garanzie[16].

Dall'altro lato, si è invece osservato che il rapporto di costante tensione tra i diritti fondamentali con l'esigenza – anch'essa di rango costituzionale – di un efficace perseguimento dei reati, rende i primi oggetto di una tutela progressiva, intesa anche come «*opportuno adeguamento all'evoluzione tecnologica e alle sfide del tempo*»[17].

Cosicché, decretare *tout court* l'inammissibilità di tali strumenti probatori causerebbe, in una prospettiva non troppo a lungo termine, la morte lenta di mezzi di ricerca della prova cardine, quali ad esempio le intercettazioni. Relegare l'oggetto di queste ultime alle tradizionali forme di comunicazione (sms, mms, chiamate) significa ridurne considerevolmente l'applicabilità[18], se si considera che i sistemi VoIP (*Voice over Internet Protocol*) hanno ormai rivoluzionato il metodo di comunicazione[19], che passa

[16] Corte Cost., 30 novembre 2009, n. 317. Anche le Sez. Un., 28 marzo 2006, n. 26795, *Prisco*, ammettono la difficoltà di «*accettare l'idea che una violazione del domicilio che la legge processuale non prevede* […] *possa legittimare la produzione di materiale di valore probatorio*».

[17] R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *Riv. It. dir. e proc. pen*., 2014, pp. 1134 ss.

[18] Nello stesso senso, L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Diritto penale contemporaneo,* 2017, n. 3.

[19] C. PARODI, *VoIP, Skype e tecnologie d'intercettazione: quali riposte d'indagine per le nuove frontiere di comunicazione?,* in *Diritto penale e processo*, 2008, n. 10, pp. 1309, 1313; S. MARIOTTI – S. TACCONI, *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni VoIP*, in *Diritto dell'Internet*, 2008, n. 6, pp. 558- 562.

attraverso la rete Internet[20]. La conversazione telefonica non si misura più in minuti, ma in *kilobyte*[21].

La cifratura del traffico telematico, a tutela della *privacy* degli utenti, sconta il prezzo della perdita di informazioni rilevanti a fini investigativi. Invece, programmi come il captatore informatico, mediante, ad esempio, l'accensione del microfono, consentono di carpire immediatamente la voce del mittente, ancor prima che il sistema VoIP utilizzato la renda indecifrabile; quanto al destinatario della comunicazione, la registrazione avviene a seguito della decodificazione del segnale, che diviene nuovamente intelligibile[22]. In altre parole, è possibile in tal modo superare il "nuovo" sistema di crittografia *end-to-end*[23], adottato anche da *WhatsApp*[24] a partire dal 2016.

Tuttavia, sembrerebbe che l'impossibilità per il gestore di "entrare" nelle conversazioni fra i due interlocutori, non comporta necessariamente l'impossibilità di deviarle all'Autorità giudiziaria, munita di apposito decreto motivato[25].

Sarebbe, dunque, preferibile, nella lunga attesa di un intervento legislativo, adeguarsi e prendere atto dell'evoluzione in corso, alla ricerca di un punto di equilibrio che resti ancorato alle garanzie ed ai valori fondamentali del nostro ordinamento giuridico, al fine di evitare una vera e propria "deriva tecnicista"[26].

---

[20] Anche i gestori di telefonia si sono adeguati al cambiamento delle abitudini comunicative, divenendo anche *Internet Service Provider*, cioè diretti gestori del traffico dati di natura telematica. Peraltro, i pacchetti tariffari offerti maggiormente competitivi sul mercato non si compongono più di sms e minuti illimitati, ma di un *quantum* di *gigabyte* sempre crescente.

[21] Comunemente indicato con il simbolo *kB*, è l'unità di misura dell'informazione, sottomultiplo del *megabyte* e del *gigabyte*.

[22] E. PIO, *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, in *Parola alla difesa*, 2016, n. 1, p.164 ss.

[23] La crittografia *end-to-end* (da "punto a punto") si basa su di un sistema di chiavi crittografiche asimmetriche. I messaggi in uscita sono protetti dalla chiave privata del mittente e possono essere decifrati solo attraverso la chiave pubblica del destinatario. In tal modo, si protegge la comunicazione dal c.d. *man in the middle*, vale a dire da eventuali tentativi di soggetti estranei di "entrare" nella comunicazione. Si passa dall'inviolabilità del *server* a quella del dispositivo.

[24] Applicazione di messaggistica istantanea per dispositivi mobili che, attraverso la connessione ad Internet, consente lo scambio tra uno o più utenti di messaggi di testo e *files* multimediali. Altri servizi di messaggistica istantanea ad uso comune sono *Telegram*, basato su *cloud*, e *Skype*, che aggiunge il sistema VoIP.

[25] F. CAJANI, *Odissea del captatore informatico*, in *Cass. pen*., 2016, p. 4143. L'A. osserva altresì che i «*gestori delle telecomunicazioni gestiscono l'informazione più importante, ossia le chiavi pubbliche e gli algoritmi crittografici presenti nel loro codice. La crittografia end-to-end prevede la possibilità di introdurre "escrew key" nel codice di programmazione, anche in modo nascosto e non facilmente rilevabile da soggetti terzi*.»

[26] L. LUPARIA osserva come «[…] *il fascino esercitato dai frutti della modernità conduce ad una loro accentuata valorizzazione ai fini del disvelamento della "verità materiale", con conseguente slittamento del baricentro del rito penale sul piano della fredda analisi dei dati tecnici, visti come segni indubitabili cui*

3. Diritti inviolabili e doveri inderogabili

Al fine di individuare un corretto bilanciamento tra esigenze investigative, finalizzate in ultimo alla repressione dei reati, e tutela dei diritti fondamentali, è anzitutto necessario individuare quali canoni costituzionali potrebbero venire compressi dall'utilizzo di tecniche informatiche quali il sopra menzionato "captatore".

Innanzitutto, massima protezione e massima garanzia vanno accordati ai diritti inviolabili dell'uomo, che la Repubblica «*riconosce e garantisce*» ai sensi dell'art. 2 della Costituzione.

La libertà personale (art. 13), il domicilio (art. 14) e la libertà e la segretezza delle comunicazioni (art. 15) sono espressamente definiti inviolabili dal legislatore costituente, che non ha escluso ipotesi derogatorie laddove quell'«*adempimento dei doveri inderogabili di solidarietà politica, economica e sociale*», pure richiesto dall'art. 2 Cost., ma spesso indebitamente trascurato, non si realizza. Ed è proprio la commissione di un fatto espressamente previsto come reato dalla legge a costituire la massima inosservanza dei doveri di solidarietà, che non ammettono alcuna deroga. Non a caso la Parte I della Costituzione è rubricata "*Diritti e doveri dei cittadini*": ogni diritto è espressamente garantito, mentre di ogni dovere ne è implicitamente presupposta la violazione nelle ipotesi derogatorie. La deroga trova giustificazione nella rottura del binomio indissolubile diritti-doveri e nella necessità di garantire la protezione dei diritti inviolabili altrui.

L'art. 13 tutela la libertà personale, intesa in senso ampio: si devono ritenere ricomprese la libertà morale e la libertà di autodeterminazione[27], nonché, indirettamente,

---

agganciare una ricostruzione del fatto commissionata, ieri agli esperti delle scienze mediche e chimico-biologiche, oggi ai tecnici dell'informatica. Per evitare l'incremento di siffatta deriva tecnicista, quindi, occorre rifugiarsi nei naturalia del processo penale, ossia in quei principi scolpiti nella cultura delle garanzie prima ancora che nella Carta fondamentale e nel codice», L. LUPARIA – G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, pp. 135, 136.

[27] A tal proposito, si veda anche il co. 4, art. 13 Cost: «*È punita ogni violenza fisica e morale sulle persone comunque sottoposte a restrizioni di libertà*». Il principio è ribadito altresì nel Codice di procedura penale tra le regole generali per l'interrogatorio (art. 64, co. 3), tra le disposizioni generali in tema di prove (art. 188) e tra i requisiti necessari ai fini dell'assunzione delle prove atipiche (art. 189). La tutela della libertà morale, quale espressione della libertà personale, si traduce in tale sede in un divieto oggettivo ed assoluto di utilizzo di metodi o tecniche idonei ad influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti.

la libertà di movimento, compromessa da eventuali restrizioni della libertà personale. Si è, infatti, autorevolmente osservato che laddove le limitazioni alla libertà di circolazione abbiano carattere generale, occorre fare riferimento all'art. 16; qualora, invece, le restrizioni riguardino specificamente un singolo individuo, la tutela si riespande nel triplice livello di garanzie di cui all'art. 13.

La formula utilizzata dal legislatore è volutamente ampia: non si limita a detenzione, ispezione e perquisizione, ma si estende a qualsiasi altra forma restrittiva della libertà, ammessa, in via condizionata solo in casi eccezionali di necessità e urgenza, tassativamente previsti.

Il domicilio, luogo di intima elezione della libertà personale e di proiezione della personalità dell'individuo, gode delle medesime garanzie previste per l'art. 13. Non a caso, la violazione di domicilio di cui all'art. 614 c.p. è inserita nella Sezione III del Capo III, recante la rubrica: "*Delitti contro la libertà individuale*". Tuttavia, si noti l'assenza nell'art. 14 di quella tendenziale espansione di tutela della libertà personale che caratterizza l'art. 13. Qui non compare la formula "qualsiasi altra restrizione della libertà domiciliare", anzi, in direzione diametralmente opposta, la Corte Costituzionale[28] ha precisato che le limitazioni testuali alle ispezioni, perquisizioni o sequestri, non costituiscono necessariamente un *numerus clausus*, poiché non è rinvenibile alcun intento di tipizzazione del legislatore costituente.

Quest'ultimo, evidentemente, non poteva tener conto delle forme di intrusioni attuali risultanti dal progresso tecnico e scientifico. In particolare, il captatore informatico installato in dispositivi elettronici portatili presenta un elevato rischio di lesione del domicilio del soggetto destinatario dell'attività d'inchiesta e dei soggetti con cui quest'ultimo interagisce, data la portabilità dell'apparecchio elettronico.

Ai fini dell'applicabilità o meno della protezione domiciliare apprestata dall'art. 14 Cost., occorre delineare i confini della nozione di domicilio.

[28] Corte Cost., 24 aprile 2002, n. 135. Si è così superato quell'orientamento secondo cui le videoriprese in ambito domiciliare sarebbero sempre e comunque costituzionalmente incompatibili a causa delle limitazioni previste dall'art. 14 Cost. Per ulteriori approfondimenti sul tema, A. MACCHIA, *I diritti fondamentali "minacciati": lo sfondo delle garanzie in costituzione*, 2017, in *Diritto Penale Contemporaneo*.

L'unico punto su cui vi è unanimità di vedute è l'insufficienza della nozione privatistica, limitata alla sede principale degli affari e degli interessi della persona (art. 43, co.1, c.c.).

Secondo taluni va individuato in «*qualunque luogo di cui si disponga a titolo privato, anche se non si tratta di privata dimora*» e malgrado la temporaneità della garanzia di intimità e riservatezza[29]. Ma, secondo la tesi dominante, confermata da una recentissima sentenza della Cassazione a Sezioni Unite[30], è necessario un rapporto di stabilità cronologicamente apprezzabile tra il luogo e l'individuo, «*tale da giustificare la tutela anche quando la persona è assente*»[31]. A tal fine, tre requisiti indefettibili devono essere integrati: 1) svolgimento di atti della vita privata[32], in modo riservato e al riparo da intrusioni esterne; 2) esistenza di un rapporto stabile, non meramente occasionale, tra il luogo e la persona; 3) inaccessibilità del luogo a terzi estranei, senza il consenso del titolare.

È controversa l'estensione della tutela costituzionale del domicilio al cosiddetto "domicilio informatico", «*lo spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, a cui viene estesa la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto*»[33]. Da un lato, quindi, si eleva tale spazio virtuale, delimitato da dati e informazioni, al rango di bene giuridico dotato di copertura costituzionale, dall'altro, il piano delle garanzie sembra traslare sull'asse più sottile della riservatezza.

---

[29] Cass., Sez. IV, 16 marzo 2000, n. 7063, *Viskovic*, in *C.E.D. Cass.,* n. 217688.

[30] Cass., Sez. Un., 22 giugno 2017, n. 31345, in *Foro It*., 2017, II, 673.

[31] Cass., Sez. Un., 28 marzo 2006, n. 26795, *Prisco*, p. 21, in *C.E.D. Cass*., n. 234270. «*Il concetto di domicilio non può essere esteso fino a farlo coincidere con un qualunque ambiente che tende a garantire intimità e riservatezza*. […] *Non c'è dubbio che il concetto di domicilio individui un rapporto tra la persona e un luogo, generalmente chiuso, in cui si svolge la vita privata, in modo anche da sottrarre chi lo occupa alle ingerenze esterne e da garantirgli quindi la riservatezza. Ma il rapporto deve essere tale da giustificare la tutela di questo anche quando la persona è assente*.». In senso conforme, la recentissima sentenza Sez. Unite 23 marzo 2017, n. 31345, cit. Per ulteriori approfondimenti vedi anche S. BERNARDI, *Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art. 624 bis c.p.*, in *Diritto penale contemporaneo* (*web*), 4 luglio 2017 (ultimo accesso: 7 ottobre 2017). Vedi *contra* Sez. VI, 16 marzo 2000, n. 7063, *Viskovic*, in *C.E.D. Cass*., n. 217688.

[32] Le Sezioni Unite forniscono un'elencazione a titolo esemplificativo: «riposo, svago, alimentazione, studio, attività professionale e di lavoro in genere» [Sez. Un., 22 giugno 2017, n. 31345, cit., p. 9].

[33] Cass., Sez. VI, 4 ottobre 1999, n. 3065, che richiama a sua volta la Relazione al disegno di legge 23 dicembre 1993, n. 547 recante **"***Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*"; Cass., Sez. V, 26 ottobre 2012, n. 42021, in *Foro It*., 2012, II, 709; Cass., Sez. V, 29 ottobre 2014, n. 52075.

In ogni caso, l'installazione di un *virus* informatico consente l'accesso ad un'enorme quantità di dati, anche strettamente personali, con una conseguente violazione del domicilio informatico del detentore del dispositivo infettato.

Quanto alla principale forma di estrinsecazione della personalità umana, la comunicazione, l'art. 15 Cost. ne assicura la libertà e la segretezza, prevedendo il rispetto di un livello minimo di garanzie che si articola su tre piani: è necessario un provvedimento dell'autorità giudiziaria, nel rispetto del principio di motivazione e della riserva di legge.

A tal proposito, in relazione alle intercettazioni, il Giudice delle leggi[34] ha richiesto la sussistenza di altre garanzie, sia di natura tecnica, volte ad assicurare il controllo sull'effettivo contenimento delle operazioni entro i limiti stabiliti dall'autorizzazione; sia di ordine giuridico, attinenti al controllo sulla legittimità del decreto di autorizzazione e sui limiti di utilizzazione nel processo del materiale risultante dalle intercettazioni. Tali garanzie "rinforzate", non operano però in relazione all'acquisizione dei tabulati attestanti il flusso del traffico telefonico di una certa utenza, in quanto la disciplina applicabile in tal caso non va ricercata nelle intercettazioni, bensì nell'art. 256 c.p.p., relativo al dovere di esibizione all'autorità giudiziaria di documenti, atti e dati riservati o segreti[35].

La tutela va intesa in senso ampio, comprensiva di tutte quelle forme intersubiettive ed attuali di comunicazione, prescindendo e dal contenuto e dal contenente. In particolare, il captatore informatico, come si vedrà[36], consente la captazione della corrispondenza elettronica contestualmente alla sua trasmissione ovvero a seguito dell'archiviazione all'interno del disco rigido.

Infine, occorre preservare il diritto di difesa, inviolabile in ogni stato e grado del procedimento ai sensi dell'art. 24, comma 2 Cost., da ogni rischio di svuotamento o svilimento.

Il preconfezionamento di prove digitali, sin dalla fase investigativa, può determinare una significativa compressione dell'esercizio del diritto di difesa. La prova verrebbe così a formarsi unilateralmente, in palese violazione con i principi del giusto

[34] Corte Cost., 4 aprile 1973, n. 34.
[35] Corte Cost. 17 luglio 1998, n. 281, § 3. Nello stesso senso anche Corte Cost., 11 marzo 1993, n. 81.
[36] Si veda cap. IV, § 5.

processo. Occorre, dunque, sin dall'inizio, porre l'interessato nelle condizioni di poter interloquire con gli organi inquirenti.

Ma il legislatore, prescrivendo l'adozione delle cautele necessarie ad assicurare la conservazione e l'integrità del dato digitale, mira, non solo a garantirne l'attendibilità ai fini dell'utilizzabilità processuale, ma anche a rendere possibile la verificabilità postuma della correttezza della procedura adottata e della conformità del dato all'originale[37].

Si attiva così, seppur *ex post* rispetto alla formazione del dato, un contraddittorio tra le parti. Contestualmente all'intervento degli organi inquirenti, «*ove si tratti di computer dell'indagato, la presenza di quest'ultimo (e quella del difensore) sul luogo dell'accertamento rende maggiore – anche dal punto di vista giuridico – il grado di resistenza di tali accertamenti in dibattimento*»[38].

Il diritto di difesa si pone in un rapporto di stretta correlazione con il diritto al contraddittorio di cui all'art. 111 Cost., nella sua duplice prospettiva soggettiva (comma 3), quale garanzia individuale, e oggettiva (comma 4), quale metodo euristico più idoneo all'accertamento. Parte della dottrina ha ribadito la necessità che entrambi i profili del contraddittorio si riflettano nella prova scientifica, altrimenti il diritto di difesa rischia di comprimersi, anziché ampliarsi, di fronte a quelle prove più insidiose per l'imputato[39].

---

[37] «*In primo luogo vi è la sacralità della conservazione dei dati originali, sia in previsione di ulteriori analisi eventualmente necessarie in futuro sia, più semplicemente, nell'ottica di garantire che, anche a distanza di mesi od anni, ci possa essere sempre la possibilità, per le parti processuali, di riferirsi e di confrontarsi con i dati originali*», G. ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA, *Sistema penale e criminalità informatica*, Milano, 2009, p. 167.

[38] F. CAJANI, *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, gennaio 2010, consultabile online al seguente sito: http://www.marcomattiucci.it/informatica_digitalforensics_l482008.php.

[39] P. TONINI, *Progresso tecnologico, prova scientifica e contraddittorio*, in L. DE CATALDO NEUBURGER (a cura di), *La prova scientifica nel processo penale*, 2007, p. 65.

CAPITOLO II

Le intercettazioni mediante l'impiego di un *virus* informatico

Sommario: 1. Le intercettazioni di conversazioni e comunicazioni mediante captatore informatico. - 2. La sentenza *Scurato*: le intercettazioni "peripatetiche". - 3. Profili critici e possibili soluzioni. – 4. L'inutilizzabilità: una sanzione adeguata? – 5. La discussa rilevanza del luogo ed i requisiti del decreto di autorizzazione. – 6. Una questione dirimente: la nozione di criminalità organizzata. – 7. Le intercettazioni di flussi informatici o telematici. – 8. Le intercettazioni di comunicazioni *Voice over Internet Protocol* (VoIP). – 9. Il caso *Occhionero*: prime applicazioni pratiche del captatore informatico alle intercettazioni telematiche.

1. Le intercettazioni di conversazioni e comunicazioni mediante captatore informatico

Il captatore informatico, definito nel precedente capitolo come quel *software* o *virus* informatico in grado di esplorare e, in alcuni casi, di "fotografare" il contenuto di un dispositivo elettronico (ad es. un telefono cellulare, un *tablet*, un *personal computer*), seguendone l'attività attraverso una sorta di *shadowing*, può costituire un mezzo attraverso il quale, tra l'altro, captare conversazioni, comunicazioni, flussi di dati, così dando luogo ad una sorta di intercettazione di conversazioni, di comunicazioni tra presenti, ovvero di flussi telematici.

Il captatore informatico può essere inserito all'interno di un dispositivo elettronico in uso alla persona soggetta a controllo e, mediante l'accensione occulta del microfono o della *webcam*, carpire conversazioni tra presenti o conversazioni a distanza; nonché copiare tutti i dati in entrata ed in uscita da e verso altri dispositivi o la rete Internet.

2. La sentenza "*Scurato*": le intercettazioni "peripatetiche"

L'ammissibilità di una simile operazione investigativa è stata affrontata dalla giurisprudenza a Sezioni Unite della Corte di Cassazione nella sentenza "*Scurato*"[40].

Secondo tale pronuncia, «*le intercettazioni di conversazioni tra presenti mediante acquisizione del controllo occulto, con "captatore informatico", di dispositivi elettronici portatili (quali smartphone, tablet, computer) in uso al soggetto intercettato, sono ammesse per i processi di criminalità organizzata per i quali, ai sensi dell'art. 13 del D.L. n. 152 del 1991, le intercettazioni nei luoghi di privata dimora sono ammesse senza limiti*».

Peraltro, tale decisione non è una monade isolata nel panorama giurisprudenziale italiano[41], ma le peculiarità del caso ivi trattato si rinvengono nella maggiore sofisticatezza del programma informatico utilizzato per la captazione, ma soprattutto nella tipologia di reato oggetto di contestazione e nel contesto spazio-temporale[42] in cui si colloca la sentenza.

Nella citata sentenza "Scurato", la Corte ha affrontato il tema relativo alla accensione del microfono di un apparecchio elettronico portatile, provocata mediante captatore informatico occultamente installato su tale dispositivo, al fine di effettuare intercettazioni tra presenti.

Ebbene, si è tentato di ricondurre tale operazione al mezzo di ricerca della prova rappresentato dalle intercettazioni e si è vagliato se potesse applicarsi o meno la disciplina

---

[40] Cass., Sez. Un, c.c. 28 aprile 2016, n. 26889, in *Foro It*., 2016, 9, 2, 491. L'indagato impugna l'ordinanza con cui il Tribunale di Palermo, in funzione del giudice del riesame, ha confermato la misura della custodia cautelare in carcere sulla base dei gravi indizi di colpevolezza emersi in relazione alla partecipazione dell'indagato all'associazione mafiosa «cosa nostra» e ai reati di estorsione aggravata e traffico di stupefacenti.

[41] Cass., Sez. V, 14 ottobre 2009, *Virruso,* in *C.E.D. Cassazione,* n. 246954, ha ritenuto legittimo il decreto del pubblico ministero di acquisizione in copia, mediante l'installazione di un captatore informatico, dei *files* memorizzati nel computer di un dipendente pubblico, collocato in un ufficio pubblico. Nel caso di specie, si è esclusa tuttavia l'applicazione della disciplina delle intercettazioni, non trattandosi di comunicazioni, e si è ritenuto applicabile l'art. 189 c.p.p.
Cass., Sez. VI, 26 maggio 2015, n. 27100, *Musumeci*, in *C.E.D. Cassazione,* n. 265654, ha ancorato l'impiego legittimo del captatore alla precisa individuazione dei luoghi nel decreto autorizzativo.

[42] L'attacco informatico alla società milanese *Hacking Team, leader* nella produzione e commercializzazione di captatori informatici, aveva rivelato l'80 per cento del codice sorgente del *software* utilizzato dalla maggioranza delle Forze di Polizia, italiane e straniere, pregiudicando importanti indagini anche nell'ambito del terrorismo internazionale.

contenuta negli artt. 266 ss. c.p.p., integrata dall'art. 13 del decreto legge n. 152 del 1991[43].

Trattavasi di procedimento per il reato di associazione per delinquere di stampo mafioso. Quest'ultimo dato non può essere negletto, dal momento che segna il limite per l'applicazione di una disciplina derogatoria anche in tema di intercettazioni.

Ebbene, l'intercettazione mediante captatore informatico non vi è dubbio costituisca, secondo la definizione comunemente accolta di intercettazione, proprio una «captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere gli altri e con modalità oggettivamente idonee allo scopo, attuata da un soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato»[44].

Cosicché dovremmo rientrare appieno nel novero della disciplina relativa alle intercettazioni.

Tuttavia, nel tal caso di specie, l'intercettazione è "itinerante" o, si vuole proporre, "peripatetica", poiché segue gli spostamenti del soggetto in possesso del dispositivo infettato, da un lato, superando i limiti delle microspie tradizionali, dall'altro, tuttavia, rischiando di dar luogo ad una pluralità di intercettazioni domiciliari, se si considera la possibilità, tutt'altro che remota, che l'intercettato si rechi nel domicilio di soggetti terzi.

Ed è proprio in relazione al domicilio che si registra il massimo discostamento della tutela apprestata dall'ordinamento nei procedimenti concernenti i delitti elencati dall'art. 266 c.p.p. e la disciplina prevista dall'art. 13 del decreto legge n. 152 del 1991.

Nel primo caso, il legislatore sembra tendere alla massima garanzia per l'indagato, laddove consente l'intercettazione domiciliare solo se vi è fondato motivo di ritenere che l'attività criminosa sia in corso di svolgimento (art. 266, co. 2); nel secondo, invece, l'esito del bilanciamento degli interessi in gioco propende a favore delle esigenze investigative, tenuto conto dell'eccezionale gravità e pericolosità dei reati di criminalità organizzata.

Dunque, il carattere "peripatetico" di tali intercettazioni e la connessa eventualità di "ingresso" nel domicilio altrui, può ritenersi compatibile, ad opinione dei Giudici di

[43] Convertito nella L. 203/1991, G. U. n. 110 del 13 maggio 1991, *Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa*.
[44] Cass., Sez. Un., 28 maggio 2003, *Torcasio*, in *Cass. pen*., 2004, p. 2094.

legittimità, con la normativa vigente, con i principi costituzionali posti a tutela dei diritti inviolabili e con la Convezione europea dei diritti dell'uomo, alla luce dei principi enunciati in *Zakharov contro Russia*[45] e in *Capriotti contro Italia*[46], soltanto nel caso in cui si proceda per delitti di criminalità organizzata; solo in tali fattispecie, infatti, è ammesso la captazione di conversazioni domiciliari anche qualora manchi il fondato motivo di ritenere che nel domicilio si stia svolgendo l'attività delittuosa.

Di qui l'affermazione del principio di diritto secondo cui «*Limitatamente ai procedimenti per delitti di criminalità organizzata, è consentita l'intercettazione di conversazioni o comunicazione tra presenti – mediante l'installazione di un ´captatore informatico´ in dispositivi elettronici portatili (ad esempio, personal computer, tablet, smartphone, ecc.) – anche nei luoghi di privata dimora ex art. 614 cod. pen., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa*».

[45] Corte EDU, Grande Camera, sent. 4 dicembre 2015. Viene ritenuto violato l'art. 8 CEDU per il mancato rispetto del canone di "qualità della legge" in mancanza di disposizioni adeguate sulle modalità autorizzative e sulla durata delle intercettazioni, nonché per la scarsa trasparenza in ordine alle modalità di conservazione o distruzione del materiale intercettato dopo la conclusione del procedimento. La normativa non soddisfa l'esigenza che le misure segrete di sorveglianza siano adottate nei limiti necessari per una società democratica.

[46] Corte EDU, sez. I, 23 febbraio 2016, riguardante un caso di intercettazione in relazione ad un reato di criminalità organizzata. Non si ritengono sussistenti elementi tali da far ritenere violato l'art. 8 CEDU.

3. Profili critici e possibili soluzioni

L'autorevolezza della fonte sopra citata, che ha ammesso entro certi limiti le intercettazioni mediante captatore informatico installato su di un cellulare, non è servita però a frenare le critiche.

E ben vengano quelle proficue e feconde, perché saranno un punto di riferimento *de iure condendo*.

Taluni[47] restano ancorati al porto sicuro della prova incostituzionale: ammetterne l'ammissibilità significherebbe «*la fine della privacy, l'annientamento degli artt. 2,13,14 e 15 Cost. e la violazione del principio europeo di proporzionalità*».

Il carattere derogatorio dell'art. 13 d.l. 152/1991 non consente di effettuare intercettazioni in ogni imprevedibile domicilio in cui sarà condotto il dispositivo infettato, «*perché darebbe luogo ad un'inammissibile autorizzazione ad una ispe-perqui-intercettazione "in bianco", cioè in qualsiasi domicilio […] si trovi il dispositivo portatile intercettato, nelle mani di chiunque lo detenga (anche terzi estranei) e con qualunque persona comunichi (anche se immune dall'intercettazione, come ad esempio il difensore o il presidente della Repubblica) su qualsiasi argomento (pure se coperto da segreto)*[48]».

Per quanto si condivida la necessità di porre in primo piano la protezione dei diritti inviolabili della persona e si apprezzi la pregnanza del termine "ispe-perqui-intercettazione", non sembra ad oggi essersi registrata un'ipotesi di impiego del captatore informatico con attivazione di tutte le funzioni che esso è in grado di svolgere. A ciò si aggiunga che non sembra potersi propendere a favore dell'inquadramento nella disciplina delle ispezioni e delle perquisizioni rispettivamente delle funzioni di *keylogger* e *screenshot*, e di acquisizione dei dati e delle unità di memoria del dispositivo controllato,

---

[47] L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi ma sbagliano la terapia (a proposito del captatore informatico)*, *Arch. pen*., 2016, n. 2, p. 348 ss.

[48] *Contra* A. CAMON, *Cavalli di Troia in Cassazione*, *Arch. nuova proc. pen.*, 2017, n. 1, p. 93. L'A. ricorda come «*alcune disposizioni consentano la sorveglianza sonora anche quando si sa in anticipo che essa è destinata a raccogliere anche conoscenze inutilizzabili; pensiamo ad un controllo telefonico disposto sull'utenza di un ambulatorio medico: possiamo star certi che ne usciranno tante conversazioni tra dottore e paziente; eppure l'ordinamento permette l'operazione e predispone un rimedio ex post, dichiarando inutilizzabili le conversazioni coperte da segreto professionale*».

a causa della diversità delle finalità e delle caratteristiche principali di tali mezzi di ricerca della prova.

Del resto, la stessa Corte Suprema non ha legittimato la disposizione di autorizzazioni "al buio", quand'anche sia astrattamente possibile seguire gli spostamenti del soggetto *target* e sospendere la captazione in caso di ingresso in un luogo di privata dimora, poiché «*sarebbe comunque impedito il controllo del giudice al momento dell'autorizzazione*»[49].

Ma, parte della dottrina fa leva proprio sulla possibilità di controllare a distanza il soggetto *target* e, di conseguenza, il dispositivo, attraverso un pedinamento elettronico o tradizionale, così da spegnere da remoto il microfono o la telecamera, a seconda dei casi, al momento dell'ingresso all'interno di un domicilio[50].

Un'altra alternativa proposta consiste nel predeterminare le fasce orarie di attivazione delle funzioni del dispositivo. In questo modo, si soddisfano, al contempo, esigenze garantistiche – di primaria importanza – ed esigenze pratiche, poiché si ottiene un considerevole risparmio di batteria[51], arginando il rischio di smascheramento delle indagini. Non a caso, sembra questa la direzione in cui si sta muovendo la riforma in atto, laddove prevede che l'attivazione del microfono avvenga solo a seguito di un «*apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto autorizzativo del giudice*».

Si consideri, inoltre, che il *virus* informatico potrebbe anche essere installato in un computer fisso, ubicato in un luogo diverso dal domicilio o all'interno del domicilio del destinatario del mezzo di ricerca della prova, in relazione al quale sono integrati i presupposti previsti dalla legge per l'effettuazione di un'intercettazione *inter praesentes*.

---

[49] Cass., Sez. Un., c.c. 28 aprile 2016, n. 26889, cit., pp. 14 e 15. Nello stesso senso, L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Diritto penale contemporaneo,* 2017, n. 3, p. 10. L'A. sottolinea che è proprio dalle obiezioni che si coglie «*la scelta più profonda della sentenza Scurato. […] le Sezioni Unite hanno reputato insoddisfacente la tutela postuma delle prerogative individuali*» derivante dall'applicazione della sanzione dell'inutilizzabilità.

[50] A. CAMON, *Cavalli di troia in Cassazione*, p. 93; A. CISTERNA, *Spazio ed intercettazioni, una liason tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni Unite*, in *Arch. pen*., 2016, n. 2, p. 331 ss.

[51] E. PIO, *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, cit., p. 161.

Allo stesso modo, il dispositivo infettato potrebbe essere un computer portatile abitualmente tenuto fermo[52].

Tuttavia, occorre altresì considerare l'ampiezza della nozione di domicilio rilevante in questa delicata materia, che riduce, ma non annulla, i casi in cui il computer bersaglio si trovi in un luogo diverso dal domicilio, latamente inteso, posto che anche il luogo in cui il soggetto esplica la sua attività lavorativa è parificato al domicilio, agli effetti della legge penale, secondo le considerazioni svolte nel capitolo precedente.

Una seconda precisazione s'impone in relazione alla tesi dottrinale su esposta. Per quanto, con una prognosi attenta, si possa ragionevolmente prevedere che il computer portatile infettato non segua gli spostamenti del soggetto *target*, non si può ignorare che rimettere la tutela dei diritti fondamentali al vago e incerto concetto di abitualità, appare una soluzione poco appagante. Vero è che il limitato spazio temporale entro il quale le intercettazioni vengono autorizzate e disposte riduce il rischio di un "cambiamento di abitudini".

Un altro orientamento[53] propone una diversa soluzione, ipotizzando un controllo giurisdizionale successivo, che attragga nella sanzione dell'inutilizzabilità le intercettazioni effettuate all'interno di un domicilio[54], vietate dalla legge. Tale linea interpretativa è stata già seguita, nonché criticata, in relazione alle video riprese all'interno di un luogo di privata dimora: il *discrimen* va individuato nel carattere comunicativo o non comunicativo dei comportamenti video ripresi. Nella prima ipotesi, le riprese visive sono ammesse nei limiti individuati dagli artt. 266 e ss., trattandosi di intercettazioni; nella seconda, invece, si tratta di prove illecite e, dunque, inutilizzabili, restando assorbita in tale sanzione processuale anche la già avvenuta lesione del diritto all'inviolabilità del domicilio.

Ma la domanda è d'obbligo: premesso che si tratta di un mezzo di ricerca della prova i cui i casi e i modi d'impiego non sono espressamente disciplinati dalla legge, che rischia di mettere a repentaglio diritti inviolabili costituzionalmente protetti da una doppia

---

[52] G. AMATO, *Reati di criminalità organizzata: possibile intercettare conversazioni o comunicazioni con un "captatore informatico"*, in Guida dir., 2016, n. 34-35, p. 79.

[53] Il riferimento è alla soluzione prospettata dalla Sesta Sezione nell'ordinanza di rimessione alle Sezioni Unite (cfr. Cass., Sez. Un, 28 aprile 2016, *Scurato*, cit., p. 14). «*Il controllo non potrà che essere successivo e riguardare il regime dell'utilizzabilità delle conversazioni captate in uno dei luoghi indicati dall'art. 614 c.p.*».

[54] Per approfondimenti sul tema delle video riprese domiciliari, cfr. M. L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni Unite*, in *Cass. pen*., 2006, pp. 3950 ss.

riserva, di legge e di giurisdizione, e che, alla luce della sentenza qui esaminata, in tanto può applicarsi senza particolari riserve e limitazioni, in quanto vi siano indizi sufficienti, sicuri ed obiettivi circa la qualificazione del fatto reato nella nozione ampia di criminalità organizzata, è adeguata la sola sanzione della inutilizzabilità, in caso di violazioni? A tale quesito, si tenterà di fornire una parvenza di risposta nel paragrafo che segue.

4. L'inutilizzabilità: una sanzione adeguata?

Quid nel caso in cui sia stata realizzata una intercettazione mediante captatore informatico al di fuori dei ristretti limiti che, ad oggi, la giurisprudenza di legittimità ha assegnato alla stessa?

La sanzione processuale applicabile dovrebbe essere quella dell'inutilizzabilità patologica di quanto raccolto, ex art. 191 c.p.p.

Tuttavia, non può negarsi la tardività di tale rimedio, in presenza di violazioni di diritti costituzionalmente protetti. E le stesse Sezioni Unite sembrano averne tenuto conto nella citata sentenza *Scurato*, sebbene non senza qualche apparente difetto di coerenza espositiva.

Infatti, se per un verso affermano l'inadeguatezza della sanzione dell'inutilizzabilità, «*riservata a gravi patologie degli atti del procedimento e del processo, e non ad ipotesi di adozione di provvedimenti contra legem e non preventivamente controllabili quanto alla loro conformità alla legge*»[55], dall'altro riprendono le osservazioni prospettate dai rappresentanti della Procura Generale nella *Memoria per la camera di consiglio delle Sezioni Unite*.

Nell'eventualità in cui si produca una lesione della dignità umana, l'ordinamento prevede la sanzione dell'inutilizzabilità, derivante dall'applicazione del principio personalistico enunciato dall'art. 2 Cost. e dalla tutela della dignità personale che ne consegue.

A ben vedere, quella che a prima vista sembra essere una *contradictio in terminis*, si risolve in realtà in una conferma di quanto inizialmente affermato.

[55] Cass., Sez. Un., c.c. 28 aprile 2016, n. 26689, *Scurato*, cit., p. 15.

Si tratterebbe, infatti, di un rimedio del tutto eccezionale, come si desume dall'inciso «*in casi estremi*», che non può che operare a posteriori, dal momento che riguarda soltanto quelle intercettazioni che, in concreto, si siano rivelate *ex post* lesive della dignità umana. I parametri di riferimento da adottare ai fini dell'accertamento della lesione, sono costituiti dalle modalità di attuazione e/o dagli esiti di "specifiche" intercettazioni.

In altre parole, in tanto l'ordinamento legittima una tutela a posteriori apprestata mediante la sanzione dell'inutilizzabilità, se ed in quanto quel pericolo di lesione dei diritti e delle libertà fondamentali, si sia concretizzato in un effettivo danno, nonostante le cautele precauzionali adottate *ex ante* nel decreto di autorizzazione.

La sanzione dell'inutilizzabilità, in conclusione, non ha natura sostitutiva, ma aggiuntiva, rappresenta un "plus" e non può considerarsi un accomodante rimedio di violazioni prevedibili ed evitabili.

5. La discussa rilevanza del luogo ed i requisiti del decreto di autorizzazione

Si è detto che, secondo la giurisprudenza di legittimità[56], l'intercettazione mediante captatore informatico può essere ammessa, seppur entro rigorosi limiti.

Peraltro, anche al fine di integrare il requisito della riserva di giurisdizione previsto dalla Carta fondamentale accanto alla riserva di legge, occorre indicare il necessario contenuto che il decreto di autorizzazione con cui il G.i.p. autorizza le intercettazioni deve avere (art. 267 c.p.p.).

Al riguardo, la sentenza "*Musumeci*"[57] aveva statuito nel senso dell'indispensabilità relativa all'indicazione del luogo, desumibile dall'art. 266, comma

[56] Cass., Sez. Un., c.c. 28 aprile 2016, n. 26889, in *Foro It*., 2016, 9, 2, 491.

[57] Cass. pen., Sez. VI, 26 maggio 2015, n. 27100, *Musumeci*, in *C.E.D. Cass.,* n. 265654. Di seguito, la massima: «*L'intercettazione di conversazioni tramite il c.d. agente intrusore, che consente la captazione "da remoto" delle conversazioni tra presenti mediante l'attivazione, attraverso il c.d. virus informatico, del microfono di un apparecchio telefonico smartphone, dà luogo ad un'intercettazione ambientale, che può ritenersi legittima, ai sensi dell'art. 266, comma secondo, cod. proc. pen. in relazione all'art. 15 Cost., solo quando il decreto autorizzativo individui con precisione i luoghi in cui espletare l'attività captativa*».

secondo. Ed ha confermato quell'orientamento giurisprudenziale secondo il quale la variazione dei luoghi in cui l'intercettazione avviene è ammessa solo se «*rientrante nella specificità dell'ambiente oggetto dell'intercettazione autorizzata*»[58].

Infatti, si sosteneva la captazione occulta non può essere ammessa in qualunque posto si trovi il soggetto. L'ammissibilità dell'intercettazione si lega alla precisa e circoscritta individuazione del luogo *ab origine*.

La successiva sentenza *Scurato* sembra aver voluto sconfessare espressamente[59] l'interpretazione espressa dalla sentenza *Musumeci*, ritenendo superflua l'esigenza di indicare un luogo specifico nel quale la captazione debba avvenire.

L'unico limite inerente al luogo, si sostiene, va individuato nell'art. 266, comma 2, che fa riferimento, nella seconda parte, ai luoghi indicati dall'art. 614 c.p., in relazione ai quali l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa. Dunque, il luogo si pone in stretta correlazione con la fondatezza della prognosi circa l'attuale svolgimento dell'attività criminosa, rilevando «*limitatamente alla motivazione del decreto nella quale il giudice deve indicare le situazioni ambientali oggetto della captazione*»[60]. Peraltro, l'art. 267, rubricato *Presupposti e forme del provvedimento*, non contiene alcuna prescrizione in relazione al luogo, nemmeno laddove disciplina un'ipotesi eccezionale, vale a dire l'adozione del decreto autorizzativo da parte del pubblico ministero: il terzo comma menziona soltanto le modalità e la durata delle operazioni tra i requisiti necessari del provvedimento.

Per quanto riguarda la giurisprudenza della Corte europea dei diritti dell'uomo, le garanzie minime che il legislatore nazionale deve apprestare in materia di intercettazioni si rinvengono nella predeterminazione dei reati che ne giustificano l'impiego, delle tipologie di comunicazioni intercettabili e dei limiti di durata, nell'attribuzione della competenza a disporre l'autorizzazione ad un organo indipendente con la previsione di un controllo giurisdizionale, nella individuazione dei casi in cui i risultati devono essere distrutti e dei limiti all'utilizzazione e conservazione degli stessi, nella definizione delle

---

[58] Cass., Sez. VI, 11 dicembre 2007, dep. 2008, n. 15396*, Stizia*, in *C.E.D. Cass.*, n. 239634; Cass., Sez. II, 15 dicembre 2010, dep. 2008, n. 4178, *Fontana,* in *C.E.D. Cass.*, n. 249207.

[59] Cass., Sez. Un*, Scurato,* cit., p. 17. La prima lacuna della ricostruzione ermeneutica della sentenza Musumeci viene individuata come segue: «*la sentenza Musumeci ha omesso di confrontarsi con il dato normativo […] ed ha piuttosto ancorato la conclusione, cui è pervenuta, alla distinzione, che non trova invece alcun aggancio normativo, tra intercettazioni tra presenti in ambienti predeterminati e intercettazioni prive di tale preventiva (individuazione e) indicazione*».

[60] *Ibidem*, p. 14.

categorie dei potenziali destinatari del provvedimento e, infine, nelle procedure da osservare per l'esame[61].

Inoltre, il termine intercettazione ambientale ha origini normative, ma è stato elaborato dalla dottrina e dalla giurisprudenza in un periodo storico in cui il mezzo tecnico attraverso cui le intercettazioni venivano effettuate era costituito dalle microspie, che necessariamente dovevano essere collocate in un determinato ambiente. Ma, come si rinviene dalle esperienze investigative, spesso risultava difficile collocarle all'interno di un domicilio, al cui interno era in corso di svolgimento l'attività criminosa, proprio perché "fisicamente presidiato". A ciò si aggiungeva il rischio di vanificare gli sforzi investigativi a causa di improvvisi cambiamenti di "ambiente" da parte dei destinatari del provvedimento. Non a caso, il legislatore non indica lo strumento con cui compiere le intercettazioni, né fornisce una precisa nozione delle stesse. È ragionevole attendersi che, in un futuro non molto prossimo, anche il captatore informatico verrà superato e sostituito da strumenti tecnologici ancora più sofisticati.

Secondo la Corte, l'utilizzo di un dispositivo elettronico "itinerante" non è altro che «*una delle naturali modalità di attuazione delle intercettazioni al pari delle microspie*».

Chiusa questa breve parentesi, il punto di riferimento per l'interprete resta il dato normativo: l'art. 266, comma secondo, non fa riferimento alle intercettazioni ambientali, ma alle intercettazioni di comunicazioni tra presenti, apponendovi una limitazione nel caso in cui si tratti di intercettazioni di comunicazioni tra presenti destinate ad avvenire nei luoghi indicati dall'art. 614 del codice penale, ai fini dell'integrazione del reato di violazione del domicilio[62]. Non si registra riferimento alcuno alla nozione di intercettazioni ambientali nemmeno nella norma speciale di cui all'art. 13 d.l. 152/1991,

---

[61] Cfr. Corte EDU, 31 maggio 2005, *Vetter contro Francia*; Corte EDU 18 maggio 2010*, Kennedy contro Regno Unito*. Sulla compatibilità della disciplina italiana con la CEDU vedi anche *Zakhrov c. Russia* e *Capriotti c. Italia* (*supra* Cap. II, § 2).

[62] Si segnala l'orientamento giurisprudenziale secondo cui in tema di intercettazioni ambientali, «*la collocazione di microspie all'interno di un luogo di privata dimora, costituendo una delle naturali modalità attuative di tale mezzo di ricerca della prova, deve ritenersi implicitamente ammessa nel provvedimento che ha disposto le operazioni di intercettazione, senza la necessità di una specifica autorizzazione. Ne consegue che la finalità di intercettare conversazioni telefoniche e/o ambientali consente all'operatore di polizia la materiale intrusione, per la collocazione dei necessari strumenti di rilevazione, negli ambiti e nei luoghi di privata dimora oggetto di tali mezzi di ricerca della prova, con il logico corollario che il P.M. non è tenuto a precisare le modalità di intrusione delle microspie in tali luoghi e che la relativa omissione non determina nullità*» (Sez. 6, n. 41514 del 25/09/2012, *Adamo*, Rv. 253805).

che consente le intercettazioni *inter praesentes*, «*anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa*». Si noti, peraltro, che l'aggettivo "fondato" non compare, a differenza di quanto previsto dalla disciplina comune.

Alla luce dell'analisi normativa, i giudici di legittimità hanno concluso nel senso che «*sarebbe errato giungere al punto di ritenere illegittima qualsiasi intercettazione tra presenti non strettamente collegata ad un predeterminato "ambiente"*».

In definitiva, quand'anche non sia possibile individuare *ex ante* nel decreto autorizzativo gli ambienti dove le registrazioni avranno luogo, le intercettazioni tra presenti sono legittime, ma esclusivamente nei casi in cui si applica la normativa derogatoria[63] ovvero, nelle ipotesi tradizionali, al di fuori della limitazione di cui all'art. 266, comma secondo. Invece, per le intercettazioni tra presenti in luoghi diversi dal domicilio, «*deve ritenersi sufficiente che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti dove essa va eseguita: l'intercettazione resta utilizzabile anche qualora venga effettuata in un altro luogo rientrante nella medesima categoria*»[64].

A conferma delle conclusioni cui è pervenuta la sentenza Scurato, è di recente intervenuta un'ulteriore sentenza della Cassazione, Sezione VI, depositata il 25 luglio 2017[65], anch'essa riguardante un procedimento *de libertate*.

Richiamando l'intero quadro dei principi enunciati dalle Sezioni Unite, la decisione si muove nel senso di operare un consolidamento dell'orientamento giurisprudenziale avviato dalla sentenza *Scurato*, contribuendo a rafforzare quella prevedibilità della decisione giudiziale cara ai giudici europei. Il merito della recente sentenza risiede, soprattutto, nella più precisa definizione dei tratti caratterizzanti il decreto di autorizzazione. In considerazione dell'invasività del mezzo tecnico adoperato, occorre rispettare un onere motivazionale rafforzato circa la sussistenza dei presupposti indicati dall'art. 267 c.p.p., fermo restando il vaglio di legittimità della Suprema Corte in ordine all'effettiva sussistenza degli stessi. È nel decreto autorizzativo che si pongono le

---

[63] Vedi anche G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, *Commento a Cass. pen., Sez. un., sent. 28 aprile 2016 (dep. 1 luglio 2016), n. 26889, Pres. Canzio, Rel. Romis, Imp. Scurato,* § 3.4, visualizzabile online al sito: www.penalecontemporaneo.it, 7 ottobre 2016. Ultimo accesso: 29 dicembre 2017.

[64] Cass., Sez. Un., *Scurato*, cit., p. 19.

[65] Cass., Sez. VI, 13 giugno 2017, n. 36874, *Romeo*, inedita. Per ulteriori approfondimenti, si veda L. GIORDANO, La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità, in *Diritto penale contemporaneo*, 2017, n. 9.

basi per un'intercettazione legittima o illegittima. L'interferenza nella sfera di riservatezza altrui si giustifica solo alla luce di gravi indizi di colpevolezza riguardanti uno specifico fatto costituente reato. Laddove tale fatto sia riconducibile nell'alveo della nozione di criminalità organizzata, su cui pure si sono soffermate le Sezioni Unite *Scurato*, se è vero che l'attività investigativa percorre, per così dire, una legale corsia preferenziale, ciò non riduce, anzi intensifica ulteriormente l'onere motivazionale del giudice, come del pubblico ministero. La qualificazione del fatto all'interno di un contesto di criminalità organizzata deve risultare ancorata a sufficienti, sicuri ed obiettivi elementi indiziari.

Il bilanciamento tra libertà e garanzie individuali ed esigenze investigative e collettive, in rapporto di costante tensione, interviene ed emerge proprio dal provvedimento di autorizzazione, che esplica, in tal modo, una fondamentale funzione di garanzia. È stato condivisibilmente osservato come sia questa l'affermazione più rilevante della decisione della Sezione VI[66].

Che l'atto investigativo sia assolutamente indispensabile ai fini della prosecuzione delle indagini (art. 267 c.p.p.) o soltanto necessario (art. 13 d.l. 152/1991), che sussistano gravi indizi o sufficienti indizi, la costante del decreto motivato di autorizzazione rimane, in ogni caso, la sua funzione garantistica, in osservanza dei principi di proporzionalità e ragionevolezza. La stessa Corte chiarisce la non necessarietà di fiumi di pagine, perché anche poche pregnanti battute sono in grado di evidenziare «*il criterio di collegamento tra l'indagine in corso e la persona da intercettare*». Dunque, anche l'individuazione del destinatario costituisce un dato fondamentale.

Adattando le peculiarità dell'agente intrusore al contenuto del decreto, è auspicabile indicare le funzioni che s'intendono attivare ed il programma utilizzato, nonché delimitare lo scopo della captazione, in modo da non legittimare attività investigative a tutto campo, aggirando il requisito imprescindibile dei gravi indizi di reato. La buona prassi si avvale di un vero e proprio protocollo che prevede, appunto, la descrizione e l'individuazione delle funzioni del *software* che verrà utilizzato, la puntuale verbalizzazione delle operazioni di installazione del *virus* utilizzato, anche a mezzo degli ausiliari di Polizia Giudiziaria, e delle procedure attuate per l'attivazione dello stesso.

---

[66] L. GIORDANO, *La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità*, in *Diritto penale contemporaneo*, 2017, n. 9.

Si prevede, infine, l'opportunità di addivenire al sequestro del dispositivo informatico attenzionato, nei limiti della materiale possibilità, al fine di garantire il rispetto del principio del contraddittorio[67], consentendo alla difesa di formulare le proprie contestazioni in merito agli esiti dell'attività captativa.

6. Una questione dirimente: la nozione di criminalità organizzata

La chiave di volta dell'impostazione ermeneutica delle Sezioni Unite Scurato è costituita dalla disciplina derogatoria prevista per i reati di criminalità organizzata dall'art. 13 d.l. 152/1991. La questione è dirimente, poiché da essa dipende la legittimità o meno delle intercettazioni effettuate mediante il captatore informatico, pur in assenza di una preventiva individuazione nel decreto autorizzativo dei luoghi attenzionati, quand'anche l'agente intrusore finisca nelle fitte maglie della privata dimora.

Ad opinione dei giudici di legittimità, il principio della riserva di legge risulta pienamente rispettato, «*proprio in virtù del più volte citato art. 13 del decreto legge 152/1991, la cui portata derogatrice (alla limitazione di cui all'art. 266, comma 2, cod. proc. pen.) non inficia in alcun modo la dettagliata disciplina*» prevista in materia di intercettazioni.

La diramazione dell'attività investigativa nel c.d. "doppio binario" può avvenire sin dalla fase delle indagini preliminari, in presenza di elementi indiziari sicuri, sufficienti ed obiettivi. Ma, al rischio di qualificazioni del fatto di reato "di comodo" consegue l'esposizione della nozione di criminalità organizzata ad eccessive dilatazioni ed indebiti piegamenti, nel perseguimento dell'ingiusto scopo di ottenere agevolazioni nella conduzione dell'attività di inchiesta, quali, ad esempio, l'autorizzazione "agevolata" a disporre le intercettazioni mediante il *software* "spia", anche in mancanza di una specifica delimitazione dei luoghi interessati.[68]

---

[67] F. CAJANI, *Odissea del captatore informatico*, in *Cass. pen*., 2016.

[68] Nello stesso senso Cass., Sez. VI, 13 giugno 2017, n. 36874, *Romeo*, inedita. La «*qualificazione dell'ipotesi associativa, che non può essere configurata come una sorta di illecito "contenitore", magari senza una specifica individuazione del ruolo e delle condotte relative ai delitti scopo dell'associazione ipotizzata, strumentalizzandone i tratti identificativi al fine di ottenere l'autorizzazione di intercettazioni*

A tal proposito, si consideri quel consolidato orientamento giurisprudenziale[69] secondo cui la valutazione circa la legittimità dell'intercettazione va parametrata al momento della richiesta e della concessione dell'autorizzazione. Di qui il seguente corollario: i risultati delle intercettazioni disposte in applicazione della disciplina derogatoria, giustificata dalla originaria prospettazione di un reato di criminalità organizzata, successivamente venuta meno nel prosieguo del procedimento, possono comunque essere utilizzati. Come ribadito anche dalla recente decisione della Sezione VI sopra menzionata, non può pretendersi di procedere a «*ad una sorta di controllo diacronico della sua ritualità [dell'intercettazione] sulla base delle risultanze derivanti dal prosieguo delle captazioni e dalle altre acquisizioni*».

In questa direzione, tuttavia, l'obbligo motivazionale stringente e rafforzato, di cui sopra si è discusso, rappresentando la minima garanzia offerta, si carica di significato e di rilevanza. L'asse si sposta tutta sul pubblico ministero, chiamato alla formulazione di un'imputazione, per quanto più possibile, corretta e coerente con gli elementi fino a quel momento emersi, e sul giudice, obbligato ad una scrupolosa analisi degli elementi prospettatigli dall'accusa in virtù del miglior bilanciamento degli interessi in gioco[70].

Quanto al contenuto della nozione di criminalità organizzata, in assenza di una specifica ed univoca definizione normativa, giurisprudenza e dottrina hanno a lungo tentato, nelle ricostruzioni interpretative, di tenersi strette al dato normativo e alle elencazioni tassative del legislatore. Tuttavia, la mutevolezza delle norme, l'influenza delle esigenze più diverse nell'emanazione delle stesse, nonché il proliferare della normativa speciale, hanno alimentato il disorientamento ermeneutico e determinato un

---

per mezzo del captatore informatico, eventualmente da utilizzare a fini di prova per reati diversi, per i quali non sarebbe stato ammesso l'impiego dello strumento.»

[69] Cass., Sez. VI, 16 maggio 1997, n. 1972, *Pacini Battaglia*, in *C.E.D. Cass*., n. 210045; Cass., Sez. VI, 1 marzo 2016, n. 21740, *Masciotta*, in *C.E.D. Cass*., n. 26692; Cass., Sez. VI, 13 giugno 2017, n. 36874, *Romeo*, inedita.

[70] Si veda anche L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Diritto penale contemporaneo,* 2017, n. 3, § 4. Secondo l'A., per scongiurare il rischio di strumentalizzazione della qualificazione giuridica associativa e di utilizzo delle risultanze probatorie per reati diversi in relazione ai quali il captatore non sarebbe stato ammesso, «*non si può che confidare nella professionalità del pubblico ministero e del giudice per le indagini preliminari.* […] *L'alternativa potrebbe essere solo la strada più semplice dell'aprioristica resistenza all'impiego del mezzo investigativo in esame*».

cambio di rotta, nella necessità di individuare, una volta e per tutte, un criterio di riferimento capace di sopravvivere ai cambiamenti legislativi.

Si vogliono qui richiamare, sinteticamente, alcune delle soluzioni proposte nel panorama interpretativo e richiamate anche dalle Sezioni Unite *Scurato*. In campo giurisprudenziale, le distinzioni operate possono ricondursi a due macro aree: la prima ricomprende quelle fattispecie riconducibili per definizione espressa del legislatore alla nozione di criminalità organizzata. Si pensi alle disposizioni previste dalla normativa speciale in materia di durata delle indagini preliminari o di intercettazioni (art. 13 d.l. 152/1991), ovvero a quelle previste dal codice di rito in tema di competenza e prerogative della Procura Distrettuale Antimafia e Antiterrorismo, contrasto tra pubblici ministeri (art. 54-*ter*), valutazione dello stato di particolare vulnerabilità della persona offesa (art. 90-*quater*), presunzione relativa di applicabilità della misura carceraria in sede cautelare.

La seconda categoria, invece, ricomprende disposizioni il cui richiamo alla nozione di criminalità organizzata avviene indirettamente, per il tramite della disciplina differenziata applicabile. Si tratta dell'art. 51, comma 3-*bis*, c.p.p. e dell'art. 407, comma secondo, lett. a) c.p.p., che contengono un elenco di reati, e che sono, a loro volta richiamati da diverse disposizioni codicistiche, con un conseguente indebolimento del principio di tassatività, come ha evidenziato la dottrina.

I reati elencati sono riconducibili, nel primo caso, ai "reati distrettuali", nel secondo, ad una «*serie composita di disposizioni incriminatrici, delle quali solo alcune sono collegate a strutture associative, mentre altre non presuppongono necessariamente il substrato di un'organizzazione criminale*»[71]. Infine, in materia di ordinamento penitenziario, si segnalano gli articoli 4-*bis* e 41-*bis* della legge del 26 luglio 1975, n. 354.

Anche in dottrina non si registra una definizione condivisa. Una parte di essa si appoggia a dati di natura socio-criminologica; altra parte, invece, cerca di restare ancorata al principio di tassatività, nel tentativo di approdare ad esiti interpretativi dal più alto grado di certezza. Taluni hanno assunto come riferimento l'art. 407, comma secondo, lett. a); altri, invece, l'art. 51, comma 3-*bis*, aggiungendovi i reati previsti dall'art. 372, comma 1-*bis* c.p.p.

[71] Cass., Sez. Un., *Scurato*, cit., p. 25.

Un orientamento intermedio si propone di distinguere i primi, definiti di "criminalità organizzata in senso stretto"[72], dai secondi, ritenuti di "criminalità organizzata in senso lato". Le Sezioni Unite non adottano una soluzione "nuova", ma decidono di seguire un indirizzo interpretativo già espresso[73], che abbraccia una nozione ampia di criminalità organizzata, comprendente «*qualsiasi fattispecie caratterizzata da una stabile organizzazione programmaticamente orientata alla commissione di più reati*». Gli unici punti fermi, nell'ambito di una nozione forse troppo ampia, nonostante gli sforzi interpretativi della Corte, sono rappresentati dalla risultante della sommatoria dei seguenti elementi: pluralità di soggetti; organizzazione stabile; esclusione del mero concorso di persone del reato.

Tuttavia, occorre innanzitutto osservare che la combinazione del primo e del terzo requisito, riduce inevitabilmente la forza dirimente del primo, la pluralità di soggetti, dal momento che è punto in comune con l'istituto del concorso di persone nel reato.

Ne discende che l'unico elemento effettivamente determinante resta la stabilità dell'organizzazione. Dunque, il confine tra il mero sodalizio estemporaneo e le associazioni criminali non presenta contorni netti e definiti, con scarsa aderenza al principio di tassatività. Peraltro, si consideri che, non solo la ricostruzione degli stessi requisiti del concorso di persone ha matrici ermeneutiche, ma altresì che lo spazio residuale tra il concorso eventuale e l'associazione delittuosa è riempito dal concorso esterno, un'ulteriore figura dai tratti non normativamente definiti.

Secondo un diffuso orientamento giurisprudenziale[74], il *discrimen* è costituito dal tasso di precisione del programma criminoso: mentre l'art. 110 c.p., nella sua funzione

---

[72] G. CONSO, *La criminalità organizzata nel linguaggio del legislatore*, in *Giust. pen*., III, 1992, p. 392. D. CURTOTTI NAPPI, *I collegamenti audiovisivi nel processo penale*, Milano, Giuffrè, 2006, p. 117. L'A. individua i delitti di criminalità organizzata in senso stretto nei delitti di cui agli «*artt. 416-bis e 630 c.p., i delitti commessi avvalendosi delle condizioni previste dal suddetto art. 416-bis, ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché i delitti di cui all'art. 74 t.u. approvato con d.P.R. 309/1990*».

[73] Cass., Sez. III, 18 giugno 2015, n. 36927, in *C.E.D. Cass*., 2016; Cass., Sez. Un., 15 luglio 2010, n. 37501, *Donadio*, in *C.E.D. Cass*., n. 247994; Cass., Sez. Un., 22 marzo 2005, *Petrarca*, n. 17706, in *C.E.D. Cass*., n. 230895.

[74] Cass., Sez. VI, 8 maggio 2013 (ud. 16 aprile 2013), n. 19783, in *Foro It.*, 2014, II, 2, 90. «*Il criterio distintivo tra il delitto di associazione per delinquere e il concorso di persone nel reato continuato va individuato nel carattere dell'accordo criminoso, che nell'indicata ipotesi di concorso si concretizza in via meramente occasionale ed accidentale, essendo diretto alla commissione di uno o più reati determinati - anche nell'ambito del medesimo disegno criminoso - con la realizzazione dei quali si esaurisce l'accordo e cessa*

estensiva, s'innesta su fattispecie delittuose realizzate sulla base di un accordo illecito occasionale, che si perfeziona con il compimento di uno o più reati predeterminati; alle associazioni criminali sono sottese pattuizioni "in bianco", dirette alla commissione di una serie indeterminata di delitti, per un periodo di tempo indefinito.

Pare scontato sottolineare il maggiore allarme sociale, rafforzato dalla continuità temporale che ne alimenta il radicamento nel territorio e la pervasività. Si tratta di una criminalità che si fa impresa, come dimostra il requisito della stabilità organizzativa, a cui l'ordinamento ricorre sia per delinearne la nozione di imprenditore, sia per finalità tributarie.

Anche sul piano europeo, si assiste ad una traduzione in chiave moderna delle associazioni criminali in termini economici: si riconosce la loro capacità di unire, al contempo, legalità e illegalità dei beni e dei servizi offerti, alterando il sistema e minando alla concorrenza, con un costo annuo stimato per le imprese di oltre 670 miliardi di euro[75]. Oltre ad essere "*una delle principali minacce per la sicurezza interna dell'Unione Europea e per la libertà dei suoi cittadini*"[76], ha assunto ormai i connotati di un'impresa commerciale transnazionale. Legittimata anche sul fronte sovranazionale, la Suprema Corte adotta una nozione ampia di criminalità organizzata, comprendente non solo i reati di cui all'articolo 51, commi 3-*bis* e 3-*quater*, «*ma anche quelli comunque facenti capo ad un'associazione per delinquere, ex art. 416 cod. pen., correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato*».

ogni motivo di allarme sociale, mentre nel reato associativo risulta diretto all'attuazione di un più vasto programma criminoso, per la commissione di una serie indeterminata di delitti, con la permanenza di un vincolo associativo tra i partecipanti, anche indipendentemente ed al di fuori dell'effettiva commissione dei singoli reati programmati».
Si veda anche Cass., Sez. VI, 5 febbraio 1998, n. 7162, in *Cass. pen*., 1999, n. 2137; Cass., Sez. VI, 12 maggio 1995, n. 9320, in *Cass. pen.*, 1995, 3387.

[75] Risoluzione del Parlamento Europeo sulla criminalità organizzata, la corruzione e il riciclaggio di danaro, adottata il 23 ottobre 2016.

[76] Risoluzione del Parlamento Europeo sulla criminalità organizzata nell'Unione Europea, adottata il 25 ottobre 2011.

7. La captazione di flussi informatici o telematici

L'introduzione dell'art. 266-*bis* del codice di rito[77] amplia il raggio applicativo dello strumento captativo rispetto a i limiti stabiliti nell'art. 266, nonostante il primo appaia, se si guarda alla collocazione sistematica, una sorta di articolazione del secondo. Ma l'estensione della possibilità di ricorrere alle intercettazioni non è indiscriminata, bensì subordinata alla sussistenza di due presupposti, legati alle modalità e all'oggetto della condotta, e all'oggetto della captazione.

Analizzando il primo profilo, l'ambito di applicazione dell'art. 266-*bis* si estende non solo ai procedimenti relativi ai reati tassativamente indicati dall'art. 266, ma anche a quelli «*commessi mediante l'impiego di tecnologie informatiche o telematiche*».

Le due fattispecie costituiscono, in tal modo, due cerchi concentrici, con un raggio applicativo della prima, l'art. 266-*bis*, più ampio.

Conseguentemente, può accadere che, nonostante un'intercettazione "tradizionale" non sia consentita, comunque possa essere disposta un'intercettazione telematica o informatica. Tuttavia, non è assente il rischio di superamento delle barriere normative, laddove si consideri l'impossibilità di escludere a monte l'acquisizione di traffico telefonico, oltre che di flusso telematico[78]. A tal proposito, anche l'apposizione di "filtri" tali da impedire l'intellegibilità delle comunicazioni vocali non costituisce che un rimedio parziale.

Taluni[79] riducono la portata innovativa della disposizione in esame.

Il riferimento, già contenuto nell'art. 266, comma primo, alle «*altre forme di telecomunicazione*», è idoneo a ricomprendere «*qualunque sistema per la trasmissione a distanza di informazioni di diversa natura*»[80]. L'unica novità apportata sarebbe costituita dall'ampliamento dei reati a cui si applica tale misura. E anche su questo punto non tutti convergono sull'interpretazione più aderente alla formula "aperta" volutamente adottata

---

[77] Legge del 23 dicembre 1993, n. 547*, Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, pubblicata in G.U. n. 305 del 30 dicembre 1993.

[78] Cfr. L. LUPARIA, *Disciplina processuale e garanzie difensive*, in L. LUPARIA – G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 163.

[79] L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, p. 82.

[80] A. CAMON, *Le intercettazioni nel processo penale,* Milano, 1996, p. 12.

dal legislatore, secondo cui la norma si riferisce non solo ai *computer crimes*, ma anche agli illeciti comuni, commessi, in concreto, mediante tecnologie telematiche o informatiche[81]. A distinguere le une dalle altre - e qui passiamo all'oggetto dell'intercettazione - sarebbe il mezzo utilizzato per la trasmissione dei dati: in caso di avvalimento della linea telefonica, televisiva o satellitare, si utilizza un sistema telematico. Viceversa, in un sistema informatico, i dati sono trasmessi via cavo o, comunque, lungo linee non telefoniche, come quelle che consentono il collegamento di varie postazioni informatiche in aree, private o pubbliche, circoscritte (c.d. LAN, *Local Area Network* o rete locale).

In ogni caso, si tratta di un'«*apprensione in tempo reale, attuata mediante l'ausilio di strumenti tecnici, di una trasmissione di dati segreta e riservata*»[82]. Dunque, resta fermo il "nucleo" essenziale della nozione di intercettazione, elaborata in via interpretativa, e, di conseguenza, risulta necessaria l'integrazione dei presupposti indicati dall'art. 267 c.p.p., ai fini dell'emissione del provvedimento autorizzativo. In merito alla restante disciplina processuale, non può negarsi una maggiore duttilità dello strumento intercettativo informatico o telematico.

Si intende far riferimento all'art. 268, comma 3-*bis*, che consente il compimento delle relative operazioni anche mediante impianti appartenenti a privati, a differenza di quanto previsto nel precedente comma in relazione alle intercettazioni di cui all'art. 266. Una deroga all'utilizzo esclusivo di impianti installati nella Procura della Repubblica è ivi consentita solo in presenza di motivate ed eccezionali ragioni di urgenza e di insufficienza od inidoneità degli impianti stessi. Una dottrina minoritaria[83] ritiene che ciò non implica l'esclusione della disciplina prevista dal comma terzo, perché il rischio di lesione della libertà e segretezza della comunicazione e il più difficile controllo dell'autorità giudiziaria circa il rispetto dei limiti fissati nell'autorizzazione, richiedono, anzi esigono, oneri motivazionali analoghi circa la necessità di ricorrere ad impianti appartenenti a privati.

---

[81] Nello stesso senso, E. APRILE - F. SPIEZIA, *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche*, Milano, 2004; SARZANA DI SANT'IPPOLITO*, Informatica e diritto penale*, Milano, 1994; A. CAMON, *Le intercettazioni nel processo penale,* Milano, 1996, p. 67. *Contra* L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, p. 82.

[82] L. LUPARIA, *Disciplina processuale e garanzie difensive,* cit., p. 162.

[83] *Ibidem*, p. 164.

Tuttavia, l'art. 271, rubricato *Divieti di utilizzazione*, menziona espressamente solo la violazione dell'art. 268, commi 1 e 3, senza far alcun riferimento, malgrado il tasso di specificità della disposizione, al comma 3-*bis*. Non si tratta di una "svista" del legislatore, per almeno tre ordini di ragioni. In primo luogo, la tassatività dei vizi processuali non consente un'interpretazione estensiva dell'art. 268, dal momento che, per quanto l'art. 191 possa essere interpretato come "norma valvola" del sistema processuale a garanzia dei diritti fondamentali, non sembra potersi applicare tale orientamento anche ai casi in cui il legislatore si è espressamente fatto carico di disciplinare specifici abusi, regolandone il relativo trattamento, come nell'art. 268.

In secondo luogo, non è stata normativamente accolta la proposta, contenuta nel disegno di legge in tema di intercettazione telefoniche ed ambientali e di pubblicità degli atti di indagine, di inserire nell'art. 266-*bis*, il comma 1-*bis*, secondo cui «*alle intercettazioni di cui al comma 1 si applicano le disposizioni relative alle intercettazioni di conversazioni o comunicazioni telefoniche*»[84]. Infine, lo stesso comma 3-*bis*, sarebbe posto nel nulla, se non si ammettesse alcuna differenza processuale rispetto alle intercettazioni *ex* art. 266.

Soluzione ideale sarebbe abbracciare un approccio intermedio, che non trascuri il dato normativo e la rilevanza del termine "anche", contenuto nel comma 3-*bis* appena citato. Il ricorso ad impianti appartenenti a privati non dovrebbe essere automatico, né, soprattutto, tradursi in un allentamento delle garanzie apprestate dal controllo "pubblico" da parte dell'autorità giudiziaria sul corretto espletamento delle operazioni opportunamente autorizzate. Il legislatore non ha *ex ante* escluso la possibilità che anche le Procure della Repubblica si dotino di impianti idonei ed adeguati all'effettuazione di intercettazioni informatiche o telematiche, in modo da non dover ricorrere ad impianti appartenenti a privati.

[84] Art. 5 del disegno di legge n. 1638, approvato il 17 aprile 2017 dalla Camera dei Deputati.

8. Le intercettazioni di comunicazioni *Voice over Internet Protocol* (VoIP)

La prassi applicativa rivela che l'art. 266-*bis* viene prevalentemente utilizzato per captare collegamenti a siti *web*, messaggi inviati tramite *email*[85] e conversazioni via *chat*. In relazione a quest'ultimo profilo, la diffusione di servizi di messaggistica istantanea ha reso possibile la comunicazione intersoggettiva attraverso la rete Internet. Tra i primi programmi basati sul sistema VoIP (*Voice over Internet Protocol*), compare senza dubbio Skype, in grado di offrire comunicazioni a distanza sia in forma scritta, trattandosi anche di un servizio di messaggistica istantanea, sia in forma orale, con potenziale osservazione contestuale degli interlocutori tramite attivazione della *webcam*[86]. Basta installare il *software* nel dispositivo portatile e creare il proprio *account* personale per accedervi.

L'affermazione secondo cui le comunicazioni VoIP tramite Skype si avvalgono della rete Internet è vera sino ad un certo punto, poiché necessita di una precisazione. È possibile effettuare anche chiamate a pagamento ad utenze telefoniche fisse o mobili, il c.d. *SkypeOut*[87]. Senza dubbio, tuttavia, l'utilizzo più comune di tale *software*, sfrutta la possibilità di effettuare, *peer to peer*, chiamate gratuite, anche internazionali, avvalendosi della sola connessione ad Internet. I vantaggi per gli utenti si moltiplicano se si aggiunge un dato fondamentale, ormai comune a quasi tutti i servizi di messaggistica istantanea[88]: la crittografia *end-to-end*[89] a protezione dei dati contenuti nelle comunicazioni da indebite intrusioni esterne (ma non si esclude, secondo taluni[90], la possibilità di convogliare il traffico direttamente all'autorità giudiziaria, previo decreto motivato di autorizzazione, e sul presupposto di un efficace collaborazione da parte del gestore).

---

[85] Il tema dell'acquisizione della corrispondenza elettronica sarà oggetto di approfondimento nel cap. IV per la labile linea di demarcazione tra la disciplina delle intercettazioni telematiche e quella relativa al sequestro.

[86] L'attivazione e la disattivazione di tale funzione avvengono dietro apposito comando azionato dall'utente. Sul sistema VoIP vedi *supra* §1.

[87] La chiamata giunge in rete fino alla nazione del destinatario, dove viene poi instradata sulla rete telefonica locale. Il passaggio dalla rete Internet alla rete telefonica rischia di non rendere possibile l'identificazione dell'indirizzo IP del chiamante, data la difficoltà di individuare il luogo in cui quest'ultimo si trova ed il dispositivo utilizzato.

[88] Fanno eccezione i servizi basati sui protocolli *standar*d SIP o H.323, rispetto ai quali l'intercettazione è sempre possibile.

[89] Sulla crittografia vedi *supra*, § 1.

[90] F. CAJANI, *Odissea del captatore informatico*, cit.

Di qui, l'estrema difficoltà di intercettare il flusso comunicativo, che ha portato allo sviluppo del captatore informatico, in grado di intercettare i dati ancor prima della loro cifratura da parte del *server*. Se la comunicazione è in uscita, i dati vengono carpiti prima della loro criptazione; viceversa, se essa è in entrata, immediatamente dopo la decodificazione, che ne consente la lettura sul dispositivo ricevente.

Ma le problematicità tecniche e giuridiche, nonché costituzionali, lo rendono uno strumento molto discusso.

Sul versante tecnico, occorre tener conto della possibilità di accedere da dispositivi diversi al medesimo *account*. Mentre le intercettazioni telefoniche si legano all'utenza telefonica, quelle che utilizzano il captatore informatico sono vincolate al dispositivo elettronico in cui il programma "spia" è installato. Ne consegue un duplice rischio legato alla "portabilità" dell'*account*: da un lato, la limitazione dell'attività d'indagine alle sole comunicazioni che il soggetto *target* effettui tramite il dispositivo infettato; dall'altro, la captazione delle comunicazioni di soggetti terzi che utilizzino quell'apparecchio elettronico per accedere al proprio *account*[91].

Si consideri, del resto, il carattere relativamente personale dell'*account*, poiché uno stesso soggetto persona fisica può possedere più identità virtuali e, quindi, più *accounts*.

Sul versante giuridico, si discute sulla disciplina processuale applicabile. Nel 2008, il legislatore aveva tentato di dare una risposta, attribuendo rilievo alla natura del gestore, per cui «*il relativo traffico è definito di natura telefonica se lo stesso è fornito da un gestore di telefonia, viceversa, il traffico ha natura telematica qualora il gestore sia un Internet Service Provider*»[92]. Ma, tale distinzione non sopravvive al confronto con l'attualità, poiché anche i gestori della telefonia mobile si sono adeguati al cambiamento degli strumenti comunicativi, divenendo essi stessi *Internet Service Provider*, cioè gestori del traffico telematico.

L'impostazione più tradizionale e garantistica, attribuisce rilievo all'oggettivo contenuto della captazione, prescindendo dal relativo canale di comunicazione. «*Non vi*

[91] La Corte di Cassazione ritiene comunque ammissibile tale prassi sulla falsariga di quanto avveniva in relazione alle intercettazioni delle utenze pubbliche (si pensi, ad esempio, alle cabine telefoniche).

[92] Art. 1, lett. d) del decreto legislativo n. 109 del 2008, *Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, pubblicato in G.U. n. 141 del 18 giugno 2008.*

è dubbio, infatti, che nella volontà del legislatore vi fosse una netta differenza di disciplina tra la conversazione vocale tra due soggetti, a prescindere dal mezzo attraverso cui essa potesse avvenire, e il trasferimento di dati, giudicato meno rilevante in un'ipotetica scala di valore, per quanto comunque degno di tutela nella parte in cui può fornire delicatissime informazioni circa l'identità dei soggetti o i riferimenti di tempo e di luogo della comunicazione stessa»[93].

L'orientamento opposto, invece, ritiene applicabile l'art. 266-*bis*[94]. Se è vero che prima dell'introduzione del suddetto articolo nel 1993, si discuteva sulla possibilità di ricomprendere nell'art. 266 le intercettazioni di comunicazioni telematiche sotto la voce "altre forme di telecomunicazione", tuttavia, l'espressa introduzione dell'art. 266-*bis* ha normativamente escluso tale possibilità. La formula in oggetto ricomprenderebbe le sole forme di telecomunicazioni, diverse da quelle informatiche, in particolare quelle coeve all'introduzione del codice di rito (ad esempio, il citofono o l'interfono per le conversazioni da intercettare in carcere)[95]. A sostegno di tale ricostruzione si pone anche un dato giurisprudenziale, che collega il mutamento dell'oggetto fisico della comunicazione telefonica al cambiamento delle relative modalità di intercettazione[96]. Si afferma altresì che «*il sistema telefonico mobile deve ormai essere considerato ai sensi dell'art. 266-bis*»[97].

In sostanza, il mezzo utilizzato per la comunicazione attrae la disciplina applicabile. Si sostiene, infatti, che l'art. 266 si riferisce implicitamente anche allo strumento impiegato, laddove richiama la contravvenzione di cui all'art. 660 del codice penale, sul presupposto che tale specifico mezzo di ricerca della prova è idoneo ad individuare taluni reati, anche privi di particolare allarme sociale.

Sinteticamente, la questione è la seguente: ai fini della disciplina applicabile, occorre attribuire prevalenza al contenuto captato, la comunicazione, oppure al canale attraverso cui i dati fluiscono? È auspicabile che qualunque sforzo interpretativo sul punto si ponga su di un piano di neutralità rispetto alla conclusione a cui perviene, nel senso che

---

[93] L. LUPARIA, *Disciplina processuale e garanzie difensive*, cit., p. 166. L'A. fa riferimento alla sentenza della Corte Cost., 11 marzo 1993, n. 81, in *Giur. It*., p. 108.

[94] Per approfondimenti sull'art. 266-*bis,* L. FILIPPI, *sub art. 266-bis*, in A. GIARDA – G. SPANGHER (a cura di), *Codice di procedura penale commentato*, I, Milano, 2010, p. 2635.

[95] F. CAJANI*, Odissea del captatore informatico*, cit.

[96] Cass., Sez., Un., 26 giugno 2008, n. 36359, in *Cass. pen*., 2009, p. 30.

[97] Cass., Sez., Un., 23 febbraio 2000, n. 6, in *Cass. pen.,* 2000, p. 2959.

non deve invertirsi quel naturale rapporto tra le premesse e il risultato, al solo fine di rispondere ad esigenze contingenti.

L'evoluzione della prassi comunicativa rischia di assottigliare ulteriormente le differenze tra l'art. 266 e l'art. 266-*bis*. Di certo, dalla formulazione delle norme si rinviene l'intenzione del legislatore di accordare una tutela rafforzata alle conversazioni o comunicazioni telefoniche rispetto a quelle informatiche o telematiche. Ma, non men vera è l'elevata difficoltà di prevedere, al tempo dell'introduzione delle disposizioni, l'attuale possibilità di effettuare chiamate attraverso un sistema telematico, che rende ancor più urgente ed impellente l'intervento legislativo.

In relazione alle comunicazioni VoIP, attribuire rilevanza al criterio dello strumento utilizzato si rivela del tutto inappagante, poiché comporterebbe un'ingiustificata disparità di trattamento. Non si può lasciare la scelta della disciplina applicabile alla decisione del soggetto chiamante, magari legata ad esigenze contingenti, puramente causali o deliberatamente elusive delle investigazioni. Il mezzo utilizzato è un elemento mutevole, al contrario, il contenuto, la comunicazione riservata e segreta, è un dato fisso e costante.

Inoltre, si potrebbe attualizzare il richiamo contenuto nell'art. 266 alle "altre forme di telecomunicazione", a differenza di quanto ritenuto dall'orientamento sopra menzionato, in modo da farvi rientrare anche le comunicazioni che si avvalgono del sistema VoIP.

In realtà, a ben vedere, la questione si ridimensiona se si considera che non sussistono differenze di disciplina particolarmente rilevanti[98], tenendo conto delle considerazioni sopra esposte (§ 7) in relazione all'art. 266-*bis*. Ciò che desta maggiore preoccupazione per l'interprete, vale a dire l'ampliamento delle ipotesi ai reati commessi mediante l'impiego di tecnologie informatiche o telematiche, non dovrebbe porre particolari problemi, dal momento che in questo caso è lo stesso legislatore ad aver preventivamente valutato la maggiore idoneità delle intercettazioni telematiche ed

[98] M. TROGU, *Le intercettazioni di comunicazioni a mezzo Skype*, in *Processo penale e Giustizia*, 2014, n. 3, p. 104. «*Non vi è dubbio che quelle in oggetto siano da catalogare come intercettazioni di comunicazioni informatiche o telematiche, la cui disciplina è sostanzialmente identica a quella dettata per le intercettazioni telefoniche o di altre forme di telecomunicazioni. Le uniche norme speciali sono contenute negli artt. 266-bis e 268, commi 3-bis, 6, 7, 8 c.p.p., ma esse non paiono sufficienti a garantire né le libertà individuali, né l'attendibilità delle prove raccolte con tale mezzo di ricerca della prova*».

informatiche ad individuare i reati commessi, data l'inadeguatezza degli altri strumenti probatori. Per quanto concerne il considerevole alleggerimento dell'onere motivazionale per il ricorso ad impianti appartenenti a privati, non assistito dalla sanzione dell'inutilizzabilità, si è già detto che esso non può tradursi in un allentamento delle maglie garantistiche del controllo giurisdizionale sulla conformità delle operazioni di captazione alle disposizioni del provvedimento di autorizzazione, che bilancia il diritto inviolabile alla libertà e alla segretezza delle comunicazioni con l'esigenza di perseguimento dei reati.

9. Il caso *Occhionero*: prime applicazioni pratiche del captatore informatico alle intercettazioni telematiche

La sentenza della Sezione Quinta della Corte di Cassazione[99], depositata il 20 ottobre 2017, costituisce una recentissima legittimazione giurisprudenziale della possibilità di installare un s*oftware* scrutatore all'interno di un dispositivo mobile, al fine di intercettare il flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi, ai sensi dell'art. 266-*bis*.

Con tale sentenza, anzitutto viene confermato il principio di diritto espresso nella sentenza *Scurato* (sulla quale, v. *supra*); ovvero, che l'intercettazione di comunicazioni tra presenti mediante l'installazione di un captatore informatico il quale segue i movimenti nello spazio dell'utilizzatore di un dispositivo elettronico (smartphone, tablet, PC portatile), è consentita nei soli procedimenti per delitti di criminalità organizzata per i quali trova applicazione la disciplina di cui all'art. 13 del D.L. n. 151 del 1991, senza necessità di preventiva individuazione ed indicazione di tali luoghi e prescindendo dalla dimostrazione che siano sede di attività criminosa in atto.

Inoltre, la sentenza *de qua* precisa che le Sezioni Unite, nella citata sentenza Scurato, non solo non escludono l'utilizzo del captatore informatico per eseguire una intercettazione (seppur coi limiti ivi indicati) ma non lo escludono nemmeno per

[99] Cass., Sez. V, 20 ottobre 2017, n. 48370 (udienza 30 maggio 2017).

effettuare una captazione di flussi telematici, benché non menzionino espressamente quest'ultima fattispecie.

Cosicché deve ritenersi legittima l'intercettazione telematica realizzata mediante captatore informatico.

Al riguardo, la Corte ribadisce che tale forma di captazione va ricondotta alla disciplina di cui all'art. 266-*bis*, escludendo invece la disciplina in materia di perquisizioni e sequestri, quando l'oggetto dell'acquisizione è costituito (anche) da un flusso di comunicazioni, che implica un dialogo intersoggettivo ed il transito bidirezionale di informazioni sui dispositivi intercettati.

Infine, si richiama quel discutibile, ma ormai invalso, orientamento giurisprudenziale[100] in virtù del quale l'onere di allegazione circa l'eventuale inutilizzabilità di taluni dati captati tramite il *virus* informatico grava sulla difesa, sulla base del principio di specificità delle impugnazioni.

Ove si accerti l'inutilizzabilità del dato, l'annullamento del provvedimento impugnato può anche non essere disposto, qualora l'elemento inutilizzabile non abbia avuto alcuna incidenza sullo stesso. A tal fine, anche il rapporto tra il dato della cui utilizzabilità si discute e la decisione oggetto di impugnazione deve essere oggetto di specificazione e chiarimento da parte del ricorrente[101].

---

[100] Tribunale di Bologna, Sez. I, 22 dicembre 2005, in *Diritto dell'internet*, 2006, p. 153. «*Dal compimento di investigazione informatiche che si discostano dalla migliore pratica scientifica non discende un'automatica inutilizzabilità del materiale probatorio raccolto. Spetta infatti alla difesa l'onere di dimostrare in che modo la metodologia utilizzata ha concretamente alterato i dati ottenuti*».
In senso conforme, Cass., Sez. II, 11 aprile 2013, n. 24925, in *C.E.D. Cass*., n. 256540; Cass., Sez. V, 4 marzo 2016, n. 26817, in *C.E.D. Cass*., n. 267889. È onere della parte curare l'acquisizione dell'atto asseritamente viziato al fascicolo trasmesso al giudice di legittimità, anche provvedendo a produrlo in copia nel giudizio in Cassazione.

[101] Cass., Sez. V, 20 ottobre 2017, n. 48370*, Occhionero*. «[…] *e, vieppiù, chiarirne l'incidenza sul complessivo compendio indiziario già valutato, sì da potersene inferire la decisività in riferimento al provvedimento impugnato (Sez. U., n. 23868 del 23/04/2009, Fruci, Rv. 243416). Il che non risulta essere stato fatto*».

CAPITOLO III

Le ispezioni e le perquisizioni "a distanza"

Sommario: 1. Cenni introduttivi. - 2. L'ispezioni informatica mediante "virus". - 3. ...ed i relativi profili problematici. - 4. (segue). L'esigenza di un livello minimo di garanzie per l'utilizzo del captatore informatico. - 5. La perquisizione *online*. - 6. …e la sua ritenuta ammissibilità. - 7. Il divieto di perquisizioni esplorative. - 8. L'inammissibilità di perquisizioni occulte.

1. Cenni introduttivi

Se il quadro di riferimento è in corso di stabilizzazione in relazione all'utilizzo del virus informatico finalizzato a captare in modo occulto una conversazione o una comunicazione tra due o più soggetti, l'incertezza interpretativa e normativa sembra regnare ancora sovrana in relazione alle altre e molteplici funzioni del captatore informatico, quale quella di ispezionare e copiare il contenuto del dispositivo elettronico sottoposto a sorveglianza.

Nemmeno il recentissimo decreto legislativo 29 dicembre 2017, n. 216[102], ha menzionato mezzi di ricerca della prova diversi dalle intercettazioni suscettibili di esperimento mediante l'installazione di un captatore informatico.

Di qui una serie di interrogativi circa l'ammissibilità o meno di una ispezione, perquisizione o sequestro eseguiti a distanza, tramite l'utilizzo di un virus informatico, che si aggiungono alle perplessità riguardanti una riforma a prima vista incompleta e ben lontana dall'apprestare le garanzie auspicate, laddove addirittura amplia il novero dei reati che giustificano il ricorso ai suddetti strumenti tecnologici.

[102] *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*. G.U. Serie Generale n. 8, 11 gennaio 2018.

La mancata menzione del captatore informatico come strumento per ispezionare/perquisire/sequestrare a distanza il contenuto di un dispositivo elettronico, in un intervento normativo che non può non aver tenuto conto del dibattito giurisprudenziale e dottrinale sul punto, può assumere una triplice lettura.

La soluzione più immediata è costituita dal "negazionismo", vale a dire dall'esclusione *tout court* di un utilizzo investigativo del captatore diverso da quello espressamente regolamentato dal legislatore.

In alternativa, ipotizzando una sorta di "gerarchia dei mezzi di ricerca della prova", si potrebbe ritenere ammissibile l'utilizzo di un tale programma informatico, dal momento che, se il legislatore l'ha espressamente previsto in una materia particolarmente delicata, quale quella delle intercettazioni, non si vede perché escluderne l'applicazione per gli altri mezzi di ricerca della prova, tradizionalmente meno insidiosi.

In questa direzione sembra essersi diretta la sentenza della Corte di Cassazione "*Occhionero*"[103], laddove afferma che il disegno di legge, allora in corso di approvazione definitiva, delega al Governo la sola disciplina inerente alle intercettazioni tra presenti perché considerata più invasiva, data la necessità di una tutela specifica per i luoghi di privata dimora. Ciò non esclude, ad opinione dei giudici, la legittimità dell'utilizzo dell'agente intrusore per le «*ulteriori intercettazioni, tra cui quelle telematiche ex art. 266-bis del codice di procedura penale*».

In terzo luogo, si potrebbe ipotizzare che l'assenza di riferimenti alle ispezioni, perquisizioni e sequestri si leghi ad una supposta completezza del sistema, data la connotazione informatica conferita a tali mezzi di ricerca della prova già con la legge 18 marzo 2008, n. 48, emanata in attuazione della Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001.

Cosicché, si potrebbe sostenere, il diritto vigente già consentirebbe l'ispezione, la perquisizione ed il sequestro attraverso l'utilizzo di un virus informatico. In particolare, la visualizzazione delle digitazioni sulla tastiera (*keylogger*) e del contenuto dello schermo (*screenshot*), consistendo in un'attività di osservazione esterna, presenterebbe

[103] Cass., Sez. V, 20 ottobre 2017, n. 48370, *Occhionero,* cit. Vedi *supra* Cap. II, § 9.

affinità con l'ispezione[104]. Mentre l'esplorazione del contenuto del disco rigido non sembrerebbe discostarsi molto dai caratteri propri della perquisizione.

Con il termine ispezione o perquisizione digitale, definita anche a distanza, da remoto o *online*, s'intende quindi quell'attività di ricerca della prova condotta mediante strumenti tecnologici, quali il captatore informatico.

Numerose le questioni che insorgono. Innanzitutto, in relazione alla realtà materiale su cui ricade l'attività dell'*inspicere* o del *perquirere*, l'ordinamento distingue tra persone, cose e luoghi, senza però fornirne una definizione.

Se si considera la contemporanea attitudine dei dispositivi elettronici ad ospitare il cosiddetto domicilio informatico[105], vien da chiedersi se l'oggetto dell'esplorazione investigativa digitale sia effettivamente individuabile in un luogo, fino ad immaginare nuove forme di captazioni 'tra presentì'.

E qui viene ad intrecciarsi il secondo principale nodo ermeneutico. Se è vero che il legislatore non fornisce una definizione precisa di intercettazione, né di ispezione, perquisizione o sequestro, è altrettanto pacifico che le intercettazioni consistono in un'attività di captazione occulta di conversazioni o comunicazioni intersoggettive, realizzata oltrepassando le barriere poste dagli interlocutori a protezione del contenuto delle stesse.

Non a caso il legislatore vi appresta maggiori cautele.

Viceversa, gli altri mezzi di ricerca della prova sono tendenzialmente conosciuti o, comunque, conoscibili dall'interessato mediante la consegna del decreto che li dispone, accompagnato, in taluni casi[106], dall'avvertimento della facoltà di farsi assistere da

---

[104] P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Processo penale e giustizia*, 2016, n. 5, p. 124. L'A. fa riferimento ad «*una sorta di atipica ispezioni online*».

[105] Si veda cap. I, § 3.

[106] Nel caso in cui si procede ad ispezioni locali o reali (art. 246), perquisizioni personali (art. 249) o locali (art. 250), incluse quelle domiciliari, una copia del decreto motivato di autorizzazione è consegnata all'interessato. Ma solo negli ultimi due casi, a cui si aggiunge l'ipotesi dell'ispezione personale, l'interessato è avvertito della facoltà di farsi assistere da persona di fiducia, purché prontamente reperibile ed idonea, a norma dell'art. 120 c.p.p. In particolare, «*non possono intervenire come testimoni agli atti del procedimento*», gli infraquattordicenni e le persone palesemente affette da infermità mentale, o in stato di manifesta urbriachezza o intossicazione da sostanze stupefacenti o psicotrope, nonché i soggetti sottoposti a misure di sicurezza detentive o a misure di prevenzione. Sulla mancata previsione della consegna di una copia del decreto motivato nel caso di ispezione personale si discuterà nel corso del capitolo.

persona di fiducia. Hanno quindi carattere palese, non occulto, e smascherano, per così dire, le indagini in corso.

Il captatore informatico è, invece, per sua natura sconosciuto all'interessato.

Anzi, la stessa installazione furtiva prevede le cautele necessarie a rendere invisibile la presenza del programma 'spia' all'interno del dispositivo infettato, che, quand'anche sia protetto da programmi antivirus, non riesce a resistere all'intrusione.

Da tali spunti di riflessione, che saranno di seguito approfonditi, discende l'evidente difficoltà di conciliare le indagini digitali a mezzo captatore informatico con la disciplina normativa vigente.

2. L'ispezione informatica mediante "virus"

Tradizionalmente, l'ispezione consiste in un'attività di osservazione diretta ed immediata di persone, cose o luoghi, così come si presentano agli occhi[107] dell'*inspiciens*, finalizzata ad «*accertare le tracce e gli altri effetti materiali del reato*»[108].

È stato autorevolmente osservato, che il codice individua anche una seconda ipotesi, in cui ci si limita alla «*constatazione di una situazione, per così dire, "indiziante"*»[109] (art. 244, comma secondo).

Il legislatore, a seguito della riforma attuata con la legge n. 48 del 2008, da taluni definita una svolta epocale, da altri, invece, ridotta a mero adattamento normativo degli istituti processuali ad una prassi già vigente, ha aggiunto un nuovo caso di ispezione, intervenendo sul comma secondo dell'art. 244 del codice di rito. In particolare, è stata interpolata la frase secondo la quale l'Autorità giudiziaria può disporre rilievi ispettivi anche in relazione a sistemi informatici e telematici.

---

[107] Sulla possibilità di realizzare un'ispezione sfruttando non solo la vista, ma tutti gli organi sensoriali, si veda G. LEONE, *Trattato di diritto processuale penale*, II, Napoli, 1961, p. 189.

[108] «*Per tracce è possibile intendere segni, macchie o impronte prodotte direttamente o indirettamente dalla condotta delittuosa; gli effetti materiali del reato, invece, sembrano richiamare alla mente le conseguenze o alterazioni di natura contundente, percussiva, ustionante, abrasiva, perforante, effrattiva che la stessa condotta può aver determinato su luoghi, cose o persone*». P. FELICIONI, *Le ispezioni e le perquisizioni*, in Trattato di procedura penale, diretto da G. UBERTIS - G. M. VOENA, Milano, 2012, p. 89.

[109] P. MOSCARINI, *Ispezione giudiziale (dir. proc. pen.)*, in *Enc. dir*., agg. II, 1998.

Più opportuna sarebbe stata la scelta di inserire l'ispezione informatica non quale continuazione del comma secondo, bensì all'interno di un autonomo comma terzo, per fugare ogni dubbio circa la possibilità di ricorrere a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica anche quando occorre accertare le tracce e gli altri effetti materiali del reato visibili (comma primo), non soltanto in caso di assenza, scomparsa, cancellazione, dispersione o alterazione degli stessi (comma secondo).

Dalla relazione di accompagnamento alla legge del 23 dicembre 1993, n. 547[110], risulta una concezione ampia del concetto di sistema informatico o telematico. Il primo comprende sia i sistemi di scrittura e di automazione d'ufficio ad uso individuale o particolare, sia complessi sistemi di elaborazione di dati in uso ad un elevato numero di utenti, distribuiti anche su di un'ampia porzione di territorio; il secondo, invece, è il risultato di collegamenti tra *computers*, o tra reti di comunicazione pubbliche e private, nazionali ed internazionali[111]. Ebbene, l'ampiezza dei confini relativi all'ispezione informatica e l'apparente facilità di adattamento del contenuto al contenitore secondo le esigenze del caso concreto e le evoluzioni delle *best practices*[112], potrebbe consentire di

---

[110] La legge, pubblicata in G. U. n. 305 del 30 dicembre 1993, reca *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*. Il tratto più innovativo è costituito dall'introduzione nel codice penale dei cosiddetti *computer crimes*: gli articoli 615-*ter*, 615-*quater* e 615-*quinquies* c.p. prevedono rispettivamente i reati di accesso abusivo a un sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

[111] G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della convenzione di Budapest sul cybercrime*, Milano, 2009, p. 194. Per ulteriori approfondimenti sulla nozione di sistema informatico vedi Cass. pen., Sez. VI, 4 ottobre 1999, n. 3067, *Piersant*i, cit., secondo cui un sistema informatico è costituito da un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, avvalendosi (anche parzialmente) di «*tecnologie informatiche, che sono caratterizzate – per mezzo di un' attività di 'codificazione' e 'decodificazione' – dalla 'registrazione' o 'memorizzazione', per mezzo d' impulsi elettronici, su supporti digitali, di 'dati', cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit, in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare 'informazioni', costituito da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. La valutazione circa il funzionamento di apparecchiature a mezzo di tali tecnologie costituisce giudizio di fatto insindacabile in Cassazione ove sorretto da motivazione adeguata ed immune da errori logici*».

[112] SWGDE (*Scientific Working Group on Digital Evidence*) *Best Practices for Computer Forensics,* versione 3.1, 2014, consultabile online: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics.

ISO/IEC 27037*, Linee guida per l'identificazione, la raccolta, l'acquisizione, la conservazione e il trasporto di evidenze digitali,* 2012. L'*International Organization for Standardization* è un'organizzazione internazionale non governativa, fondata a Ginevra nel 1947, che spesso collabora con l'*International Electrotechinical Commission*, a cui aderiscono 60 paesi. A livello europeo, si segnala l'*Electronic Evidence*

ricondurvi anche quella condotta mediante captatore informatico, così sottoponendo la medesima alla disciplina di cui all'art. 244 c.p.p.

In particolare, poi, si deve osservare che l'ispezione di un dispositivo quale un cellulare, un *tablet*, un *personal computer* presenti connotati più personalistici, che 'ambientali'. Infatti, il dispositivo oggetto di controllo costituisce sì uno "spazio", sia pure virtuale, ma pur sempre dai confini illimitati ed in grado di accogliere un enorme numero di dati e informazioni personali, caratterizzati ciascuno da un diverso grado di riservatezza. Pertanto, data la prevalenza di caratteri individualisti, sembra corretto ipotizzare che l'ispezione a distanza, come l'omologa perquisizione, costituisca un particolare caso di ispezione personale.

Tale ragionamento segue una prassi già affermatasi prima dell'introduzione della legge n. 48/2008: così come, prima della riforma, le norme in tema di ispezione, perquisizione e sequestro, ancorché forgiate su elementi fisici, venivano adattate per realizzare tali attività in relazione a siti *web, file di log*, dati o programmi informatici; allo stesso modo, si potrebbe ipotizzare di fornire una copertura normativa alle ulteriori funzioni del captatore informatico ricorrendo alle norme già esistenti.

3. …e i relativi profili problematici

Tuttavia, l'operazione ermeneutica volta a ricomprendere tra le ispezioni informatiche, ammesse dalla legge, anche quella realizzate mediante captatore si scontra con almeno tre obiezioni, di carattere letterale, sistematico e costituzionale.

In primo luogo, l'art. 244 consente «*rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici*», riferendosi all'oggetto dell'attività ispettiva, senza alcun riferimento al mezzo di espletamento della stessa.

La citata legge n. 48/2008 sembra essere ritagliata sui reati informatici "puri", in cui il dispositivo elettronico costituisce oggetto materiale del reato ovvero cosa pertinente al reato (reati informatici "spuri"), o, comunque, sui reati comuni commessi mediante le

Guide, elaborata nel 2013 (con un aggiornamento nel 2014) grazie al contributo del Consiglio d'Europa e del Consiglio dell'Unione Europea.

tecnologie informatiche. Inoltre, la *ratio* della suddetta legge, nonché della Convenzione di Budapest, di cui la legge è attuazione, va individuata nel contrasto alla criminalità informatica, anche mediante la previsione di misure per l'acquisizione di dati digitali conformi alle tutele e alle garanzie previste dalla Convenzione del Consiglio d'Europa del 1950 e alla Convenzione internazionale delle Nazioni Unite sui diritti civili e politici del 1966 (art. 15).

Il raggio di applicazione del captatore informatico è, invece, più ampio, dal momento che non si limita ai reati informatici, per quanto possa rivelarsi utile anche in tale contesto, ma si estende a qualsiasi reato, con il limite del divieto di indagini informatiche *ad explorandum*, del tutto slegate da una *notitia criminis*[113].

A ciò si aggiunga il carattere occulto delle ispezioni a mezzo captatore informatico, che non sono né conosciute, né conoscibili dall'interessato.

Infine, dal punto di vista costituzionale, occorre chiedersi se l'invasività dello strumento non sia tale da impedirne un vaglio positivo di compatibilità con la Carta fondamentale.

Mentre le intercettazioni "peripatetiche" presentano il rischio che il dispositivo portatile del soggetto *target* entri nel domicilio di soggetti estranei alle indagini, violando indebitamente il domicilio altrui e realizzando intercettazioni *inter praesentes* non autorizzate e, di conseguenza, illegittime; nel caso delle ispezioni e, soprattutto, delle perquisizioni a distanza, l'intrusione occulta nel sistema informatico o telematico pone problemi di invasività "interna", nel senso che la minaccia della lesione di diritti fondamentali si proietta esclusivamente nei confronti del fruitore del dispositivo.

Come si è osservato nel paragrafo precedente, l'ispezione elettronica incide più che su di una "cosa", *i.e.* il sistema informatico o telematico, su di un "luogo", avente carattere virtuale; ovvero sul c.d. "domicilio informatico".

Punto d'incontro tra l'art. 2 e l'art. 14 Cost., esso rappresenta la progressione della tutela dei diritti fondamentali dell'individuo.

Il concetto di domicilio informatico è stato elaborato a partire dall'introduzione dei reati informatici con la legge del 23 dicembre 1993, n. 574, quale bene giuridico

[113] Vedi *infra* cap. III, § 7.

tutelato dagli artt. 615-*bis* e 615-*ter* c.p.[114], collocati tra i delitti contro l'inviolabilità del domicilio. Dalla relazione di accompagnamento emerge che lo scopo dell'introduzione delle nuove fattispecie incriminatrici è quello di tutelare i sistemi informatici o telematici, in quanto «*espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del codice penale*».

È stato giustamente osservato che «*il parallelismo con il domicilio, bene eminentemente privato e personale, coglie solo parzialmente il contenuto dell'interesse all'esclusione di terzi da determinate "sfere di disponibilità e rispetto", create e rese fruibili dalla tecnologia informatica*»[115].

Dunque, il domicilio informatico è un *quid pluris* rispetto al luogo fisico protetto dall'art. 14 Cost. attraverso una doppia riserva, di legge e di giurisdizione, poiché si lega anche alla riservatezza, tutelata a sua volta all'interno dell'art. 2 Cost.

A tal proposito, la Corte Costituzionale tedesca ha coniato un nuovo diritto fondamentale alla "garanzia della segretezza e integrità dei sistemi informatici"[116], meritevole di una tutela rafforzata: occorre un provvedimento motivato dell'autorità giudiziaria, a cui è demandato il controllo circa il corretto utilizzo dello strumento investigativo, in conformità con il principio di proporzionalità. La compressione dei diritti fondamentali si può giustificare solo alla luce del perseguimento di uno scopo legittimo, attraverso misure idonee e necessarie al raggiungimento dello stesso. Occorre, infine, prevedere misure tecniche che garantiscano la cancellazione dei dati irrilevanti e inutilizzabili.

---

[114] Si noti la collocazione sistematica dei reati informatici nel Capo III, rubricato "*Delitti contro le libertà individuali*", del Titolo XI, "*Delitti contro la persona*". Per ulteriori informazioni sulla legge 547/1993 si veda la nota n. 5 di questo capitolo.

[115] L. PICOTTI*, Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Cedam, Padova 2004, p. 180.

[116] *Bundesverfassungsgericht,* 27 febbraio 2008, BVerGE 120, 274 ss. Nel caso di specie la Corte, pur dichiarando l'illegittimità costituzionale dell'art. 5, co. secondo, n. 11 della legge sulla protezione della Costituzione del Nord Reno-Westfalia, non esclude *tout court* la possibilità di utilizzare un *software* in grado di monitorare e accedere in segreto ai sistemi informatici collegati ad Internet. Per un approfondimento sul tema si veda R. FLOR, *Brevi riflessioni a margine della sentenza del 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 sostanziale,* in *Riv. trim. dir. pen. ec*., 2009, p. 697 ss.; F. AGHIRÒ*, L'ammissibilità delle intercettazioni telematiche (on-line Durchsuchungen) al vaglio del Budesgerichthof: il caso dei c.d. Bundestrojaner*, in *Arch. pen*., 2008, n. 1, pp. 271-272.

In Italia, come in Europa, il bilanciamento tra esigenze investigative e diritti individuali risulta tutt'altro che agevole, ma mentre in Germania già nel 2008 e, nuovamente, nel 2016[117] si discuteva circa la legittimità costituzionale di una legge che espressamente prevede l'utilizzo di un *software* a fini investigativi, in Italia, ancora si auspica un intervento legislativo, completo e puntale, nonostante gli sforzi recenti. Un ruolo di supplenza è stato svolto da giurisprudenza e dottrina, che hanno tentato di riempire il vuoto normativo. In virtù dell'interpretazione dell'art. 8 CEDU da parte della Corte Europea dei diritti dell'uomo, il requisito della previsione legislativa delle ingerenze nella vita privata può essere integrato non solo dalla legge, ma anche dalla giurisprudenza, purché siano garantite al cittadino prevedibilità e conoscibilità della fonte. Ma, tale interpretazione trova applicazione in relazione agli ordinamenti di Common Law.

In ogni caso, le garanzie poste a tutela del diritto alla riservatezza informatica vanno ricercate non solo all'interno della Costituzione, dove incontrano il limite della riserva di legge e di giurisdizione, ma anche nella normativa europea, che impone il rispetto dei principi di proporzionalità e di stretta necessità della misura rispetto alle finalità legittime perseguite.

Tale tutela rinforzata deriva dalla struttura stessa del diritto alla riservatezza informatica, che costituisce, rispetto al diritto alla riservatezza e al diritto all'inviolabilità del domicilio, un cerchio concentrico dal raggio maggiore.

La tutela apprestata dagli art. 2 e 14 Cost., singolarmente considerati, risulta inadeguata. Infatti, il concetto di domicilio informatico ben si inserisce in entrambi: dall'art. 2, norma a carattere aperto, mutua la riservatezza; dall'art. 14, la spazialità della

---

117 Bundersverfassungsgericht, I Senato, 20 aprile 2016 - 1 BVR 966/09, 1 BVR 1140/09. La Corte afferma la compatibilità con i diritti costituzionali del ricorso a misure di sorveglianza occulte a fini di contrasto al terrorismo internazionale. Tuttavia, in taluni punti, la legge federale "*Bundeskriminalamtgesetz* - BKAG" viola il principio di proporzionalità. Da quest'ultimo dovrebbero derivare i seguenti corollari: estendere la raccolta segreta di dati personali a soggetti estranei alle indagini solo in casi particolari; informare le parti interessate dell'avvenuto espletamento delle misure, ponendole in condizione di attivare un controllo giurisdizionale; tutelare adeguatamente i soggetti titolari di un segreto professionale; esercitare in modo trasparente il potere investigativo sotto il controllo dell'autorità giurisdizionale; introdurre una previsione normativa che preveda la cancellazione dei dati personali raccolti dopo il loro utilizzo; obbligo di relazionare al Parlamento e all'opinione pubblica.
Per ulteriori approfondimenti, si veda A. VENEGONI - L. GIORDANO, *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*. (*web*), 8 maggio 2016 (ultimo accesso: 17 gennaio 2018).

proiezione virtuale dell'essere umano, che impone la tutela rinforzata della doppia riserva legislativa e giurisdizionale.

Cosicché, l'ispezione a distanza, così come la perquisizione *online* di cui si tratterà a breve, incontrano un ostacolo costituzionale difficile da superare nella protezione di diritti fondamentali dell'individuo, individuati negli art. 13, 14, 15 Cost., nonché nell'art. 2 Cost.

4. (segue). L'esigenza di un livello minimo di garanzie per l'utilizzo del captatore informatico

Alla luce di quanto sopra, la soluzione astrattamente più corretta e preferibile, in piena aderenza al principio di legalità e tassatività, sembrerebbe allora consistere nel ritenere inammissibili mezzi digitali di ricerca della prova non espressamente regolamentati dal legislatore in ciascuna delle loro componenti.

Tuttavia, occorre dare conto di una prassi indisturbata, che da più di un decennio vi fa ricorso, come dimostra il panorama del diritto vivente italiano, di cui sono riportati alcuni esempi nei paragrafi seguenti.

Di qui il tentativo di uno sforzo interpretativo, che, prendendo atto dell'ormai diffuso utilizzo del captatore informatico per la realizzazione di ispezioni, perquisizioni e sequestri a distanza, miri comunque ad apprestare quantomeno un livello minimo di garanzie, nell'attesa di un intervento del legislatore.

Ed allora, si dovrebbero rendere le ispezioni *online* atti palesi e così attivare *ab origine* un efficace contraddittorio con l'interessato. Se non si vuole retroagire al sistema inquisitorio del passato, dominato dalla segretezza e dalla raccolta unilaterale della prova, è necessario riconoscere al difensore, d'ufficio o di fiducia, il diritto di preavviso almeno ventiquattro ore prima del compimento dell'operazione (art. 364, comma terzo), a meno che sussista un fondato motivo di alterazione delle tracce o degli altri effetti materiali del reato.

Nei casi di assoluta urgenza, quando dal ritardo potrebbe ragionevolmente derivare un pregiudizio alla ricerca e all'assicurazione delle fonti di prova, il pubblico

ministero può procedere anche prima che siano trascorse le ventiquattro ore, indicando i motivi specifici della deroga e dandone tempestivo avviso al difensore, che ha, in ogni caso, la facoltà d'intervento.

In altre parole, le ispezioni a distanza in tanto possono essere eventualmente espletate, in quanto la difesa sia posta sin dall'inizio nelle condizioni di poter interloquire e siano, in ogni caso, adottate procedure idonee a garantire la conservazione dei dati originali e ad impedirne l'alterazione.

5. La perquisizione *online*

La tradizionale distinzione tra l'*inspicere* e il *perquirere* resta ferma anche in relazione ai nuovi mezzi di ricerca della prova digitale.

Mentre l'ispezione si limita all'osservazione esterna delle tracce e degli altri effetti materiali del reato, la perquisizione, anche se a distanza, consiste in una ricerca attiva del corpo del reato e delle cose pertinenti al reato[118], quand'anche l'involucro che le contiene sia costituito da un sistema informatico o telematico.

Tra le sue funzioni, occorre ricordare la possibilità per il captatore informatico di visualizzare le digitazioni sulla tastiera (*keylogger*) e il contenuto dello schermo (*screenshot*).

Fin tanto che ci si limita a guardare all'esterno dell'involucro digitale, prendendo atto dell'esistenza di determinati documenti, dati o programmi informatici, si rientra nella c.d. *online surveillance*.

Qualora, invece, si 'entri' nel sistema informatico, aprendo, ad esempio, il documento, allora si ha uno sconfinamento nella perquisizione a distanza.

Secondo taluni, la differenza tra i due istituti digitali risiede nella presenza o meno di credenziali d'accesso a protezione del sistema. Nel primo caso, si tratta di una perquisizione; nel secondo, di un'ispezione, visto che il dato normativo (art. 247, comma 1-*bis*) contiene una precisazione con riferimento alle sole perquisizioni: possono essere disposte ancorché il sistema informatico sia *«protetto da misure di sicurezza*». Ma tale

[118] Ai sensi dell'art. 253, comma secondo, «*sono corpo del reato le cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo*».

impostazione non può essere accolta, poiché rimette l'applicazione di una certa disciplina alla scelta arbitraria dell'utente di proteggere o meno con una *password* i dati digitali. Né dalla mancata predisposizione di credenziali di accesso si può dedurre una minore aspettativa di riservatezza.

Le perquisizioni *on line*, a distanza, vanno peraltro tenute distinte dalle più tradizionali perquisizioni informatiche. Ovvero, da quelle aventi semplicemente ad oggetto un sistema informatico, per le quali l'art. 247, comma 1-*bis* impone l'adozione di «*misure tecniche dirette ad assicurare la conservazione dei dati digitali e ad impedirne l'alterazione*».

In primo luogo, le perquisizioni informatiche *tout court* presuppongono un rapporto diretto tra l'autorità giudiziaria e l'interessato, ove presente, a cui è consegnata copia del decreto motivato che dispone la perquisizione personale o locale, con l'avviso della facoltà di farsi assistere da persona di fiducia, con l'unico limite della reperibilità e dell'idoneità della stessa *ex* art. 120 c.p.p.

L'atto procedimentale viene ad essere un'anticipazione, seppur in scala ridotta, del processo quale *actus trium personarum*.

La limitazione della libertà personale o domiciliare è quindi conosciuta o, almeno, conoscibile dall'interessato, che è posto nelle condizioni di presenziare all'attività di indagine e, eventualmente, di interloquire (si pensi alla richiesta di consegna).

Invece, le perquisizioni a distanza a mezzo captatore informatico hanno carattere occulto e vengono volutamente espletate all'insaputa dell'interessato.

In secondo luogo, le perquisizioni informatiche, come quelle tradizionali, sono rivolte al passato, nel senso che hanno ad oggetto dati, informazioni, programmi informatici o tracce comunque pertinenti al reato già precostituiti e storicizzati. Viceversa, tale precostituzione si affievolisce con riferimento alle perquisizioni digitali, che si proiettano verso il futuro, perché possono captare non solo dati in tempo reale, ma anche dati *in fieri*, se non contenute entro limiti temporali contingenti previsti dal decreto di autorizzazione.

Un'ulteriore differenza risiede nei rapporti cronologici con il sequestro materiale. Ai sensi dell'art. 252, «*le cose rinvenute a seguito di perquisizione sono sottoposte a sequestro con l'osservanza delle prescrizioni degli artt. 259 e 260*».

Un'attenta dottrina ha osservato che, in relazione al dato digitale, si ha un'inversione temporale tra perquisizione informatica e sequestro[119].

Quest'ultimo anticipa l'attività di ricerca delle tracce digitali, che avviene "a freddo", dopo l'acquisizione del dispositivo elettronico e la realizzazione di una copia forense dei dati[120]. Ma, tale affermazione necessita di una precisazione. In caso di rischio di perdita irreversibile dei dati o in caso di impossibilità di sequestro del dispositivo elettronico, si procede con una *Live forensic analysis*[121], che rende il sequestro materiale un'ipotesi residuale. In relazione alla perquisizione da remoto, invece, si ripristina il naturale rapporto tra perquisizione e sequestro materiale del dispositivo elettronico, che potrebbe rivelarsi, anche in tal caso, non necessario.

Pertanto, la perquisizione a distanza presenta una natura ibrida, a metà strada tra le intercettazioni, con cui condivide il carattere occulto, e la perquisizione informatica, con cui condivide l'oggetto su cui ricade l'attività di ricerca, un sistema informatico o telematico, caratterizzato da dati immateriali, di cui occorre garantire l'originalità, l'integrità e l'immodificabilità.

Ed allora, non è agevole l'inquadramento delle "perquisizioni 2.0", ovvero di quelle realizzate a distanza.

Ad opinione di chi scrive, sembrerebbe trattarsi di un appostamento informatico, rientrante quindi nell'attività di *online surveillance* e non di una vera e propria perquisizione. Ma, l'opinione prevalente aderisce alla tesi opposta: l'acquisizione in copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira costituisce una "perquisizione", seppure *online*[122].

---

119 L. LUPARIA, *La ratifica della Convenzione cybercrime del Consiglio d'Europa. Legge del 18 marzo del 2008, n. 48. I profili processuali*, in *Dir. pen. proc*., 2008, p. 720; E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 154.

120 Cass., Sez. V, 16 gennaio 2018 (ud. 27 novembre 2017), n. 1822: «*una modalità conforme alla legge, che mira a proteggere, nell'interesse di tutte le parti, l'integrità e l'affidabilità del dato così acquisito*»

121 A differenza della analisi *post-mortem*, l'analisi è effettuata in tempo reale mentre il sistema è attivo, onde evitare la perdita irreversibile di informazioni che conseguirebbe allo spegnimento dell'apparecchio elettronico. Si consiglia di acquisire i dati in ordine di volatilità decrescente, più precisamente dal più volatile al meno volatile (registri di sistema, memoria *cache*, *files* di sistema temporanei, *file* di log da remoto, configurazione fisica del sistema informatico e, infine, il contenuto dei supporti di memoria).

122 P. FELICIONI, *L'acquisizione da remoto di dati digitali nel processo penale*, cit., p. 124.

6. … e la sua ritenuta ammissibilità

La Corte di Cassazione, con la sentenza "*Virruso*"[123], fornisce il primo approccio giurisprudenziale italiano al ricorso ad un captatore informatico (*gosth*) al fine di carpire i *files* presenti nella memoria del *computer* interessato, sia quelli già esistenti al momento in cui è iniziata l'operazione, sia quelli *in fieri*.

Nel caso di specie, l'utilizzo di tale *software* da parte della Polizia di Stato poggiava esclusivamente sul decreto del pubblico ministero e la Corte di Cassazione ha ritenuto legittima tale operazione.

Com'è evidente, il virus informatico impiegato, seppur privo della odierna multifunzionalità, realizzava un monitoraggio continuo ed occulto del sistema informatico interessato, protrattosi per otto mesi e sottratto ad un controllo giurisdizionale.

La difesa si era opposta alla ricostruzione operata dai giudici di primo grado, che avevano concluso a favore della sussunzione di tale attività investigativa nell'alveo delle prove atipiche ai sensi dell'art. 189.

In particolare, aveva sostenuto la difesa, non si tratterebbe di prove atipiche, bensì di intercettazioni telematiche.

Di conseguenza la disciplina applicabile, l'art. 266-*bis*, avrebbe richiesto un provvedimento autorizzativo motivato del giudice delle indagini preliminari, dietro richiesta del pubblico ministero. Ma, oltre che di prove inutilizzabili *ex* art. 191, in quanto acquisite in violazione della disciplina normativa, si sarebbe trattato, ancor prima, di "prove incostituzionali"[124], perché acquisite in spregio dei diritti fondamentali di cui agli artt. 14 e 15 Cost.

Ma la Corte di Cassazione non ha accolto le doglianze difensive.

---

[123] Cass., Sez. V, 14 ottobre 2009, n. 16556, in *C.E.D*, n. 246954.

[124] Per ulteriori approfondimenti sul tema si veda P. MOSCARINI, *Lineamenti del sistema istruttorio penale*, cit., p. 148.

L'oggetto dell'attività captativa – hanno osservato i Giudici di legittimità – va individuato in un «*una relazione operativa tra microprocessore e video del sistema elettronico, ossia un flusso unidirezionale di dati confinato all'interno dei circuiti del personal computer*».

In sostanza, l'attività autorizzata dal pubblico ministero, «*consistente nel prelevare e copiare documenti memorizzati sull'hard disk dell'apparecchio*», non ha ad oggetto un flusso di comunicazioni, caratterizzato da un dialogo intersoggettivo[125].

Tale argomento vale anche ad escludere la violazione dell'art. 15 Cost., mancando una forma di comunicazione[126]. I giudici di legittimità hanno negato altresì l'esistenza di un pregiudizio al diritto all'inviolabilità del domicilio, considerando dirimente l'ubicazione del computer fisso in un ufficio pubblico comunale, accessibile non soltanto all'imputato e agli altri impiegati, ma anche, sia pure con determinate cadenze temporali, al pubblico degli utenti ed al personale delle pulizie, *«insomma una comunità di soggetti non particolarmente estesa, ma nemmeno limitata o determinabile a priori in ragione di una determinazione personale dell'imputato*»[127].

Tuttavia, se si considerano le riflessioni su esposte con riferimento al diritto alla riservatezza informatica[128], pare evidente che tale argomentazione risulta forse troppo riduttiva. Si conferisce rilievo esclusivamente all'ubicazione fisica del dispositivo elettronico, «*così obliterando la tutela costituzionale del domicilio informatico, che […] può rappresentare addirittura qualcosa di più personale e intimo del domicilio tradizionale*»[129].

---

[125] Cass., Sez. Un., 23 febbraio 2000, n. 6, in *Il Foro Italiano*, 2000, n. 10, 529. Per flusso di comunicazioni s'intende «*la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un ricevente, da un soggetto ad altro, ossia il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici*».

[126] Cass., Sez. V, 14 ottobre 2009, n. 16556, in *C.E.D*, n. 246954, sostiene che «*quanto riprodotto in copia non era un testo inoltrato e trasmesso col sistema informatico, ma soltanto predisposto per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario*».

[127] *Ibidem*.

[128] Vedi *supra* cap. III, § 3.

[129] P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale*, cit., p. 132. Nello stesso senso, M. TORRE, *Il virus di stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali: mezzi di ricerca della prova*, in *Dir. pen. proc*., 2015, n. 9, p. 1167.
Sul punto si veda anche L. BATTINIERI, *La perquisizione online tra esigenze investigative e ricerca atipica della prova*, in *Sicurezza e Giustizia*, 2013, n. 4, p. 45. Secondo l'A. «*ciò che conta al fine di valutare se tale mezzo atipico di ricerca della prova presenti punti di conflitto con il diritto costituzionale alla inviolabilità del domicilio non è la collocazione spazio-materiale del sistema informatico bensì la possibilità o meno di ritenere che l'apparato interessato costituisca proiezione del domicilio fisico del privato che ne fa uso, conclusione da escludere nei soli casi in cui, ad esempio, si tratti di un computer messo a disposizione di*

Sebbene la sentenza sia abbastanza risalente nel tempo, l'elaborazione del concetto di 'domicilio informatico' è coeva all'introduzione dei c.d. *computer crimes* con la legge 23 dicembre 1993, n. 547.

La sentenza, tuttavia, non tiene conto dell'interesse individuale al godimento, al controllo e all'utilizzo esclusivo dei dati contenuti nel sistema informatico o telematico in uso al destinatario dell'attività d'inchiesta[130]. Una compressione del diritto alla riservatezza informatica non può essere giustificata soltanto sulla base del decreto del pubblico ministero, a maggior ragione se la protrazione del monitoraggio copre un arco temporale piuttosto lungo, come è avvenuto nel caso di specie, con scarsa aderenza al principio di proporzionalità della misura.

Infine, si vuole analizzare un ultimo profilo. Quella che la stessa Corte di Cassazione definisce un'attività di prelevamento e copia di documenti memorizzati sull'*hard disk* del dispositivo elettronico, sembra presentare un'affinità con il sequestro digitale o, quantomeno, con la perquisizione, in linea con l'opinione prevalente secondo cui l'acquisizione in copia dei dati rientra nella perquisizione *online*. In ogni caso, si tratta di *online search*[131]. Di conseguenza, la disciplina in astratto applicabile non rientrerebbe tanto nell'art. 189, come ritenuto dai giudici, né nell'art. 266-*bis*, come sostenuto dalla difesa, bensì nell'art. 247, comma 1-*bis*.

Tuttavia, occorre considerare che anche tale norma può rilevarsi inadeguata, laddove si tratti di un appostamento informatico occulto e prolungato nel tempo, che comprende sia i dati già esistenti, sia i dati elaborandi.

In conclusione, un profilo di atipicità non può negarsi, ma ciò non giustifica un monitoraggio indiscriminato, disancorato ad un provvedimento motivato del giudice, in mancanza del quale i risultati raggiunti avrebbero dovuto essere dichiarati inutilizzabili.

---

una platea indifferenziata di utenti e destinato alla effettuazione di operazioni non aventi alcuna attinenza con la sfera strettamente personale di chi ne fruisce».

[130] R. FLOR, *Phishing, identity theft, e identity abuse*: *le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen*., 2007. L'A. definisce la riservatezza informatica come «*l'interesse esclusivo, giuridicamente riconosciuto, di godere, disporre e controllare le informazioni, i procedimenti, i sistemi e "spazi" informatizzati e le relative utilità*».

[131] Sulla differenza tra *online search* e *online surveillance* si veda cap. I, § 2.

Ma tale indirizzo interpretativo non sembra essere stato oggetto di critiche in giurisprudenza, come dimostra il caso "*Bisignani*", relativo alle indagini sull'associazione massonica P4[132].

Nonostante la richiesta del pubblico ministero al giudice delle indagini preliminari di autorizzare l'utilizzo di un captatore informatico per realizzare sia un'attività di *online search* sia di *online surveillance*, il g.i.p. ritiene di aderire all'orientamento sposato dalla sentenza *Virruso* in relazione alla seconda attività. Pertanto, ha emanato il decreto di autorizzazione solo in relazione alla funzione di attivazione del microfono e della video camera, che avrebbe consentito un'intercettazione tra presenti con una "cimice informatica".

Invece, con riferimento alla funzione di acquisizione e di estrazione dei dati digitali contenuti nel dispositivo elettronico interessato, è stato ritenuto sufficiente il decreto del pubblico ministero.

Sebbene sia condivisibile l'esclusione di tale attività dalla disciplina delle intercettazioni, ciò non giustifica di per sé la non necessarietà di un decreto autorizzativo, dal momento che il *software* impiegato senza dubbio incide sulla sfera di riservatezza individuale, nella sua proiezione virtuale e a-fisica.

7. Il divieto di perquisizioni esplorative

Con una più recente sentenza, pronunciata dalla Corte di Cassazione con riguardo al caso *Ryanair*, è stato fissato un limite invalicabile per le perquisizioni c.d. *online*, ponendo un punto fermo rivelatosi tutt'altro che scontato.

La Corte di Cassazione[133] conferma l'annullamento, già disposto dal Tribunale del riesame, del decreto del pubblico ministero di perquisizione e sequestro delle

[132] Le indagini sono state avviate nel 2007 (procedimento penale n. 39306/2007 R.G.N.R., mod. 21). Secondo la Procura della Repubblica presso il Tribunale di Napoli gli imputati avrebbero creato un sistema di alleanze finalizzato all' «*illecita acquisizione di notizie e di informazioni, anche coperte da segreto, alcune delle quali inerenti a procedimenti penali in corso nonché di altri dati sensibili e personali al fine di consentire a soggetti inquisiti di eludere le indagini giudiziarie ovvero per ottenere favori o altre utilità*».

[133] Cass., Sez. IV, 24 maggio 2012 (udienza 17 aprile 2012), n. 19618, in *Cass. pen*., 2013, p. 1523 ss.

credenziali d'accesso al sistema di prenotazione *online* dei voli della nota compagnia aerea.

Lo scopo investigativo mirava all'identificazione preventiva dei c.d. 'ovulatori', ovvero dei corrieri internazionali di droga, sulla base del mero sospetto derivante da una serie di indici sintomatici, quali le prenotazioni *last-minute*, la brevità del soggiorno, l'orario notturno dei viaggi.

La Corte di Cassazione ha ritenuto legittima la decisione con cui il Tribunale del riesame aveva annullato il provvedimento di perquisizione e sequestro delle credenziali di accesso al sistema informatico di prenotazione dei voli "*online*" di una compagnia aerea onde identificare per tempo - in base ad una serie di parametri sintomatici desumibili dalle modalità di prenotazione dei voli - i passeggeri sospettabili di fungere da corrieri internazionali di stupefacenti (c.d. ovulatori), trattandosi di provvedimento preordinato non tanto ad acquisire elementi di conoscenza in ordine ad una o più "*notitiae criminis*" determinate, quanto a monitorare in modo illimitato, preventivo e permanente il contenuto di un sistema informatico onde pervenire all'accertamento di reati non ancora commessi, ma dei quali si ipotizzi la futura commissione da parte di soggetti da individuarsi; né al riguardo può essere invocato l'art. 248, comma secondo, cod. proc. pen., novellato dalla legge n. 48 del 2008 - per il quale l'autorità giudiziaria e gli ufficiali di polizia giudiziaria da questa delegati, per rintracciare le cose da sottoporre a sequestro o accertare altre circostanze utili ai fini delle indagini, possono esaminare presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici - il quale laddove richiama le banche non può che riferirsi agli istituti di credito e non già alle banche dati, per giunta in continuo aggiornamento automatico, presso qualsiasi altro ente o struttura privata o pubblica, tanto più che il termine banca-dati non risulta mai adoperato dall'ordinamento giuridico italiano che utilizza la diversa dizione di sistema informatico o telematico.

Il caso fa emergere il sottoprodotto non desiderato dell'utilizzo di un mezzo di ricerca della prova non disciplinato dal legislatore, con un' inevitabile erosione del principio di legalità e di riserva di legge: ad applicazioni erronee della disciplina processuale vigente, nel tentativo di adattarla all'evoluzione tecnologica, rischiano di far seguito serie compromissioni dei diritti fondamentali dell'individuo, che non solo prescindono da un attento bilanciamento degli interessi in gioco, ma che rischiano

addirittura di tradursi in uno stravolgimento dei livelli minimi di garanzia. Quei «*principi scolpiti nella cultura delle garanzie, prima ancora che nella Carta fondamentale e nel codice, i quali […] possono essere sufficienti per risolvere le questioni connesse al nuovo fenomeno delle indagini informatiche*[134]», sembrano essere stati dimenticati in questa vicenda.

In particolare, non si è tenuto conto della distinzione tra l'oggetto su cui ricade l'attività di ricerca (nel caso in esame, il sistema informatico o telematico) e l'oggetto della ricerca stessa, il corpo del reato o le cose pertinenti al reato («*dati, informazioni, programmi informatici, o tracce comunque pertinenti al reato*»). Tali due elementi si trovano in rapporto di contenente a contenuto, per accedere al quale occorre imprescindibilmente individuare un *fumus commissi delicti*, che dovrà risultare dalla motivazione del decreto con cui si dispone la perquisizione.

Nel caso *de quo*, invece, l'obiettivo illecito che si tentava di perseguire consisteva in un monitoraggio preventivo ed illimitatamente esplorativo del sistema di *booking online*, in cui compaiono, anche, e soprattutto, i dati relativi a soggetti del tutto estranei alle indagini. Ma – e questo è il dato più sconcertante – non poteva dirsi avviato per nessuno, nemmeno per i potenziali sospetti, un vero e proprio procedimento penale, in quanto mancava *ab origine* una notizia di reato. Non può ammettersi un'inversione dell'ordine consequenziale delle fasi procedimentali, il cui punto di partenza è costituito dall'iscrizione di una notizia di reato nel registro di cui all'art. 335 c.p.p., dal quale decorre il termine di durata delle indagini preliminari.

Il decreto motivato, pertanto, non può limitarsi ad indicare il titolo del reato, ma deve specificare la norma penale che s'intende violata dal fatto concreto, a sua volta individuato dalle circostanze di tempo, di luogo e di azione.

L'ordinamento non può legittimare una "denaturalizzazione" dei mezzi di ricerca della prova, ridotti a mezzi di ricerca della *notitia criminis,* volti ad accertare reati non ancora commessi. Secondo i giudici di legittimità, «*è da escludere un preventivo ed indefinito monitoraggio del sistema predetto in attesa dell'eventuale e futura comparsa del dato da acquisire*[135] *a base delle indagini: si verrebbe altrimenti ad integrare un nuovo ed anomalo strumento di ricerca della prova, con finalità nettamente esplorative,*

---

134 L. LUPARIA, *Disciplina processuale e garanzie difensive*, cit., p. 128.

135 F. CORONA*, Perquisizioni di sistema informatico per le prenotazioni dei voli online: i dati devono essere già presenti*, in *Sicurezza e Giustizia*, 2015, n. 3.

di mera investigazione (paragonabile alle intercettazioni), che nulla ha a che fare con la perquisizione».

Tuttavia, sembra opportuno osservare che l'"abnormità' dell'attività posta in essere nel caso in esame non consente nemmeno un paragone con le intercettazioni, la cui disciplina è di gran lunga più garantista, dal momento che richiede gravi (o almeno sufficienti) indizi di reità, nonché l'assoluta indispensabilità per la prosecuzione delle indagini, non per l'avvio delle stesse.

In conclusione, vige un assoluto divieto di indagini digitali *ad explorandum*, che si avvalgono illegittimamente di mezzi digitali di ricerca della prova, pur in assenza di un *fumus commissi delicti.*

8. L'inammissibilità di perquisizioni occulte

Contrariamente a quanto sostenuto dalla giurisprudenza sinora esposta, ragioni garantistiche sembrerebbero imporre che la perquisizione a distanza mediante l'impego di un captatore informatico debba essere ritenuta inammissibile.

L'ordinamento non può legittimare, mediante un mero decreto autorizzativo, forme atipiche di intrusione nella sfera individuale.

L'installazione di un programma informatico in grado di esplorare i dati contenuti all'interno del sistema informatico attenzionato realizzerebbe un'attività di ricerca della prova altamente intrusiva, assimilabile alle perquisizioni personali. Infatti, il ragionamento sopra esposto circa il potenziale inquadramento dell'ispezione a distanza nell'alveo dell'ispezione personale può ripetersi anche per le perquisizioni, atteso che il domicilio informatico sembra costituire un'appendice della personalità individuale.

Di conseguenza, l'esecuzione delle operazioni sarebbe incompatibile con il rispetto della dignità umana[136], previsto dall'art. 249, comma secondo, con una formula analoga a quella già prevista per le ispezioni personali (art. 245, comma secondo).

[136] Sulle criticità espresse dalla dottrina in merito all'inciso «*e, nei limiti del possibile, del pudore di chi vi è sottoposto*» si rinvia a P. BALDUCCI, *Perquisizioni*, in *Enc. dir.*, IV, Milano, 2000, p. 982. La dignità è un concetto più ampio del pudore. Ne discende l'irragionevolezza dell'imposizione di limitazioni in relazione al pudore, mentre alla dignità sarebbe assicurata una tutela piena.

Pertanto, le uniche forme legittime di perquisizione sono quelle riconducibili nell'alveo delle perquisizioni informatiche di cui all'art. 247 comma 1-*bis* c.p.p.

La disciplina sottesa alla novella intervenuta, in materia di ispezioni e perquisizioni, con la legge n. 48/2008 presenta un duplice vantaggio.

Da un lato, tale disciplina àncora il ricorso alle perquisizioni digitali alla sussistenza di un *fumus commissi delicti*, scongiurando illegittime degenerazioni dei mezzi di ricerca della prova in strumenti di acquisizione della *notitia criminis* (cfr. cap. III, § 7). Dall'altro, risponde ad un'esigenza di necessaria conformità al diritto inviolabile di difesa in ogni stato e grado del procedimento[137] ed al principio del contraddittorio.

A tal proposito, a differenza di quanto osservato in tema di ispezioni, è prevista la consegna della copia del decreto motivato, sia che l'attività abbia ad oggetto persone sia che abbia ad oggetto luoghi.

Vige, infatti, un principio di equipollenza[138] in tema di perquisizioni in relazione alla conoscibilità da parte dell'interessato dell'operazione lesiva che sta per essere condotta.

Tale trasparenza non si riviene, invece, in relazione alle perquisizioni *online* che non possono essere condotte all'insaputa dell'interessato, per quanto si tratti di atti "a sorpresa".

Verrebbe meno la garanzia dell'interazione dell'interessato con l'autorità giudiziaria, in applicazione del principio della richiesta di consegna.

La consegna di certo non potrà avvenire materialmente, quando si tratti di dati, informazioni o programmi contenuti in un sistema informatico o telematico. Ma, l'eventuale collaborazione dell'interessato a fornire all'autorità giudiziaria gli elementi rilevanti ai fini delle indagini in corso, può senza dubbio consentire un rilevante contenimento della lesione della sfera individuale, poiché, ai sensi dell'art. 248, comma primo, «*non si procede alla perquisizione, salvo che si ritenga utile procedervi per la completezza delle indagini*». In tal modo, potrebbe ritenersi assorbito *ab origine* il rischio di acquisizione di dati strettamente personali, che nulla hanno a che vedere con le indagini.

---

[137] Vedi *supra* cap. I, § 3.

[138] E. BASSO, *Art. 249*, in *Commento al nuovo codice di procedura penale*, coordinato da M. CHIAVARIO, II, Torino, 1990, p. 715.

L'operazione può essere parimenti evitata se si consente all'autorità giudiziaria o agli ufficiali di polizia giudiziaria di esaminare atti, documenti e corrispondenza, nonché dati informazioni e programmi informatici presso banche, intese, com'è ovvio, quali istituti di credito. Tuttavia, sul punto si è dovuta pronunciare la Corte di Cassazione[139], che ha negato la possibilità di estendere il concetto di banca di cui all'art. 248, comma secondo, fino a ricomprendervi le banche-dati[140], come invece sostenuto dal ricorrente, il Procuratore della Repubblica presso il Tribunale di Pisa.

In conclusione, l'imprescindibile esigenza di rispettare i principi costituzionali impone all'interprete il divieto di legittimare intrusioni nella sfera di riservatezza virtuale dell'individuo sulla base di un mero decreto del pubblico ministero.

L'interessato deve poter avere contezza dell'imminente frapposizione da parte dell'autorità giudiziaria al libero esercizio del diritto alla riservatezza informatica.

Pertanto, non parrebbero ammissibili perquisizioni occulte, incompatibili con il diritto inviolabile di difesa in ogni stato e grado del procedimento.

Ne consegue la necessità di prevedere strumenti volti a garantire la conoscibilità della lesione in atto, come previsto dalla disciplina attualmente vigente attraverso la consegna di una copia del decreto motivato che dispone l'operazione.

139 Cass., Sez. IV, 24 maggio 2012, n. 19618, cit. (§ 7).

140 Sul punto si veda G. BONO, *Il divieto di indagini ad explorandum include i mezzi informatici di ricerca della prova*, in *Cass. pen.*, 2013, n. 4, pp. 1530-1531.

CAPITOLO IV
I SEQUESTRI DIGITALI "STATICI" E "DINAMICI"

Sommario: 1. Il sequestro informatico. - 2. …ed i relativi aspetti problematici. - 3. Il sequestro mediante l'utilizzo di un captatore informatico. - 4. Circa l'ammissibilità di un sequestro informatico mediante captatore informatico. - 5. La captazione della posta elettronica e delle *e-mail* in "bozza" mediante *virus* informatico. 6. L'equiparazione giurisprudenziale delle *e-mail* alla prova documentale

1. Il sequestro informatico

Tradizionalmente, il sequestro è successivo alla perquisizione, con cui condivide, non a caso, l'oggetto: il corpo del reato e le cose pertinenti al reato necessarie all'accertamento dei fatti.

Ma, come si è in parte accennato in precedenza, quel tradizionale rapporto di logica consequenzialità tra perquisizione e sequestro cede, anzi, si capovolge di fronte all'immaterialità e all'immanenza dell'universo digitale.

Quando si tratta di *computer crimes* in senso stretto o di *computer-related crimes*, senza dubbio il dispositivo elettronico costituisce lo strumento di commissione del reato o l'oggetto su cui ricade l'attività criminosa. Pertanto, è pacifica la sua sottoposizione a sequestro.

Invece, in relazione ai reati comuni, il sequestro del *computer* e, come spesso si è verificato, delle periferiche ad esso collegate, può rivelarsi eccessivo e sproporzionato rispetto alla finalità perseguita dagli organi inquirenti.

Cosicché, in alternativa all'apprensione fisica del dispositivo, la c.d. "*live data forensic analysis*" consente la realizzazione di una copia legale sul posto da parte di soggetti qualificati, seguendo gli schemi dell'accertamento tecnico irripetibile.

L'interessato, pur rimanendo nella disponibilità del dispositivo, è costretto a subire una restrizione irreversibile e prolungata dell'area di "riservatezza digitale", nella quale possono entrare non solo gli organi inquirenti, ma anche il difensore.

L'orientamento giurisprudenziale e dottrinale[141] più garantistico è nel senso di evitare, per quanto possibile, l'apprensione fisica dell'apparecchio elettronico. Pertanto, nei casi in cui elementi immateriali, non *res* tangibili, costituiscono oggetto d'interesse investigativo, il sequestro materiale dell'involucro che li contiene può essere sostituito dalla copia dei dati contenuti nel dispositivo attenzionato.

Tale soluzione, del resto, è già espressamente prevista dall'art. 254-*bis* c.p.p.[142], aggiunto dall'art. 8, comma quinto, della legge del 18 marzo 2008, n. 48, in tema di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni. In tale particolare fattispecie, al fine di evitare l'interruzione del servizio fornito agli utenti da tali gestori, si prevede che l'Autorità giudiziaria possa disporre il sequestro dei dati digitali non mediante l'apprensione fisica dei dispositivi elettronici che li contengono, ma attraverso la copia di tali informazioni su un adeguato supporto.

Che l'acquisizione di dati, informazioni o programmi informatici mediante copia di essi su di un supporto informatico sia assimilabile ad un'operazione di sequestro può desumersi implicitamente anche dall'art. 256, comma primo. Il dovere di consegna di quanto richiesto ai soggetti di cui agli artt. 200 e 201 con il decreto di esibizione può avere ad oggetto elementi probatori digitali contenuti in un supporto materiale (CD, DVD, *pen drive*).

Un'ulteriore conferma sul punto si rinviene nella relazione esplicativa della Convenzione di Budapest, adottata dal Comitato dei ministri del Consiglio d'Europa, dove si chiarisce che "sequestrare" significa «*prendere il mezzo fisico sul quale i dati o*

---

[141] L. LUPARIA*, Disciplina processuale e garanzie difensive*, cit., pp. 176-177. «*La sottoposizione a vincolo del computer, infatti, da un lato priva il soggetto di uno strumento essenziale della vita contemporanea (o costringe una società a interrompere la propria attività economica), dall'altro, risulta lesiva del principio di pertinenza delle indagini rispetto all'addebito provvisorio, giacché vengono acquisiti una serie di dati digitali del tutto irrilevanti per la constatazione dell'illecito*».

[142] Per un approfondimento sull'art. 254-*bis* si veda S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, n. 4, pp. 966-967; A. MACRILLÒ, *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. Int*., 2008, pp. 513-514.

le informazioni sono registrati oppure fare e trattenere una copia di tali dati o informazioni»[143].

In altre parole, nonostante il mutamento dell'oggetto della ricerca probatoria, che non si identifica più nella "cosa" materiale, bensì nella "cosa" digitale, resta fermo il sequestro quale mezzo di ricerca della prova. L'effetto finale è, infatti, il medesimo: l'indisponibilità giuridica della cosa sequestrata[144]. Più correttamente, si viene a delineare una disponibilità giuridicamente e giudizialmente condivisa dei dati digitali ed un conseguente "spossessamento" del titolare del diritto all'uso esclusivo degli stessi.

Pertanto, si può riconoscere non solo la configurabilità di un sequestro, ma anche la maggiore insidiosità di quest'ultimo, laddove non si garantisca all'interessato la restituzione dei supporti contenenti le duplicazioni dei dati. Altrimenti, si corre il rischio di un loro indebito utilizzo in altri procedimenti e per un tempo indefinito, in patente elusione delle garanzie difensive[145].

A tal proposito, si è giustamente riconosciuto, non senza iniziali resistenze giurisprudenziali[146], l'interesse ad impugnare il provvedimento di sequestro, quand'anche la restituzione sia già avvenuta[147]. Dalla lettura congiunta dell'art. 258, commi primo e secondo, «*si ricava che, nonostante la riconsegna, sull'oggetto possono permanere limitazioni di natura probatoria che impongono un vincolo di indisponibilità, tradotto nell'obbligo di fare menzione, nelle copie estratte, del sequestro esistente sull'originale. Pertanto, […] non può dirsi che alla riconsegna materiale della cosa si determini automaticamente il "dissequestro", specialmente quando se ne conservi copia*»[148].

---

[143] Cass. pen., Sez. Un., 7 settembre 2017 (ud. 20 luglio 2017), n. 40963, *Andreucci*, in *C.E.D. Cass*., n. 27049701; Cass., Sez. II, 10 novembre 2017 (ud. 18 ottobre 2017), n.51446.

[144] A. DALIA, *Sequestro penale,* in G. VASSALLI (a cura di), *Dizionario di diritto e procedura penale*, Milano, 1986, p. 939. «*Pacifico l'effetto mirato precipuo: l'indisponibilità giuridica (e per lo più anche reale) della cosa sequestrata*».

[145] G. SCHENA, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, in *Cass. pen.* 2016, n. 1, p. 302.

[146] Si veda Cass., Sez. VI, 10 giugno 2015 (ud. 24 febbraio 2015), n. 24617, n. 264094. Si nega la configurabilità di un sequestro e, di conseguenza, il diritto all'impugnazione in sede di riesame, in relazione alla «*duplicazione o stampa su carta di dati presenti nel computer, come qualsiasi copia di atti*».

[147] Cass., Sez. Un., 20 luglio 2017, n. 40963, *Andreucci*, in *C.E.D*. Cass., n. 270497.

[148] G. SCHENA, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, cit., p. 302.

2. … ed i relativi aspetti problematici

La residualità del sequestro materiale dell'apparecchio elettronico, per quanto sia idonea a consentire la tutela della proprietà e la prosecuzione dell'attività d'impresa, se l'utilizzo del dispositivo si lega all'esercizio di un'attività commerciale o professionale, non è tuttavia in grado di assorbire le questioni inerenti ad un'adeguata tutela dei diritti individuali.

In particolare, l'acquisizione in copia degli elementi probatori digitali è suscettibile di arrecare pregiudizio al diritto alla riservatezza informatica, alla libertà e segretezza della corrispondenza[149] ed al diritto di difesa, nonché, in taluni casi, alla tutela del segreto professionale.

Le esigenze di salvaguardia si amplificano quando i titolari dei diritti esposti a rischio lesione si identificano in soggetti terzi estranei alle indagini.

Allo stato attuale dell'evoluzione tecnologica, sembra doversi dare atto dell'inesistenza di programmi informatici capaci di selezionare il materiale probatorio potenzialmente utile alle indagini contenuto all'interno della memoria del dispositivo.

Conseguentemente, il rispetto dei principi di proporzionalità e di adeguatezza della misura impone la ricerca di vie alternative alla copia integrale del disco rigido, contenente presumibilmente anche un gran numero di dati strettamente personali, privi di qualunque legame pertinenziale col reato.

Le garanzie di difesa sono strettamente correlate al rispetto del diritto alla privatezza della proiezione virtuale della persona.

Quanto prima si attiva il contraddittorio con l'interessato, tanto minore sarà la lesione della sfera di riservatezza elettronica.

[149] Il diritto inviolabile costituzionalmente protetto dall'art. 15 Cost. rischia di essere pregiudicato in relazione all'acquisizione della corrispondenza elettronica, altrettanto contenuta nell'*hard disk*. Si veda *infra* § 4.

Il destinatario del provvedimento può utilmente collaborare con l'autorità giudiziaria, indicando i documenti effettivamente idonei all'accertamento dei fatti.

In tal modo, si evita l'acquisizione totale del contenuto del disco rigido.

Se, ciononostante, dati personali irrilevanti vengono comunque acquisiti, l'ordinamento non può non fornire un rimedio, seppur successivo, che potrebbe essere individuato nell'eliminazione degli stessi dal materiale probatorio e nella conseguente distruzione, così come accade per le intercettazioni.

Un'attenta dottrina[150] ha evidenziato la necessità di prevedere che la copia legale venga depositata non solo presso la segreteria del pubblico ministero - con facoltà per la difesa di prenderne visione e di estrarne copia -, ma anche presso la cancelleria del giudice per le indagini preliminari, al fine di contenere il rischio di ricerca di nuove *notitiae criminis*[151] da parte del pubblico ministero. In un'apposita udienza-stralcio, convocata dal g.i.p. nelle forme dell'incidente probatorio, si dovrebbe procedere alla selezione del materiale rilevante per le indagini, destinato a confluire nel fascicolo del dibattimento[152].

Ma, ancor prima, appare doveroso selezionare *ex ante* il materiale pertinente, ad esempio, attraverso la predisposizione delle parole chiave da inserire all'interno dell'elaboratore[153], similmente a quanto accade in relazione all'esame testimoniale.

La diversità del sequestro informatico rispetto al sequestro, per così dire, 'tradizionale', impone la predisposizione delle opportune cautele, nel tentativo di realizzare il miglior bilanciamento possibile degli interessi in gioco. Ne consegue un provvedimento di sequestro informatico molto più dettagliato in punto di motivazione, non potendosi più accettare «*provvedimenti genericamente finalizzati all'esplorazione di*

---

150 P. TROISI, *Sequestro probatorio del computer e segreto giornalistico*, in *Dir. pen. proc.,* 2008, n. 6, pp. 689 ss.

151 Cass., Sez. I, 16 febbraio 2007, n. 237430, *Pomarici*, in *Cass. pen*., 2008, p. 2956 ss., con nota di A. LOGLI, *Sequestro probatorio di un personal computer*. *Misure ad explorandum e tutela della corrispondenza elettronica*, cit. Il pericolo di trasformazione dell'attività investigativa in un'attività di ricerca di ulteriori *notitiae criminis* «*si fa probabile, anzi, diventa 'presunto'*»..

152 F. IOVENE, *Perquisizioni e sequestro di computer: un'analisi comparatistica*, cit. «*Se durante l'incidente probatorio si dovessero rinvenire prove o il corpo di un reato diverso, il pubblico ministero dovrebbe procedere all'iscrizione della relativa notizia di reato. Una volta terminato l'incidente probatorio*, […] *i files irrilevanti, in tutte le copie che se ne posseggono, andrebbero distrutti o restituiti al proprietario. Ciò permetterebbe altresì di risolvere la questione della mancanza di interessa ad impugnare il provvedimento di sequestro nel caso in cui il bene sia stato restituito*». Nello stesso senso, G. SCHENA, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, cit., p. 306.

153 F. M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen*., 2012, n. 2, p. 711.

tutti i dati digitali contenuti all'interno dell'hard disk, attraverso l'apertura (e quindi la lettura) di tutti i files in esso contenuti con riserva di selezionare (compito delegato alla p.g.) soltanto alla fine quelli "utili" alle indagini».[154]

In sostanza, come si è già osservato in tema di perquisizioni, anche con riferimento al sequestro di dati digitali, non è ammesso alcun piegamento dei mezzi di ricerca della prova a mezzi di ricerca della notizia di reato, in assenza di un *fumus commissi delicti*[155].

In tal caso, opera una sorta di presunzione assoluta di violazione del principio di proporzionalità tra la misura adottata e lo scopo perseguito, in patente contrasto con l'art. 8 CEDU e con il *dictum* più volte ribadito dalle Sezioni Unite[156].

Parimenti utili alla preselezione del materiale probatorio da acquisire si rivelano le ispezioni e le perquisizioni informatiche e digitali, i cui risultati possono certamente contribuire alla delimitazione dell'area di estensione del sequestro.

Piuttosto che procedere con una sproporzionata clonazione dell'intero disco rigido, verranno copiati esclusivamente i dati rilevanti all'accertamento del reato, del suo autore e delle circostanze. Si rispetta così il vincolo di pertinenza col reato, a cui molto spesso non è legato l'intero *hard disk*, ma soltanto alcuni dei dati in esso contenuti, non suscettibili di separazione *ex ante* dai dati strettamente personali.

Dunque, l'individuazione del materiale probatorio oggetto d'interesse deve precedere l'attività di acquisizione dei dati[157], la quale investirà solo gli elementi *ex ante* pertinenti al fatto criminoso, comprendenti anche quelli in qualsiasi modo connessi ad esso o indirettamente rilevanti, secondo la nozione ampia di pertinenza elaborata dalla giurisprudenza[158].

---

[154] F. M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen*., 2012, n. 2, p. 709.

[155] Cass., Sez. VI, 2 aprile 2014, n. 33229, *Visca*, in *C.E.D Cass*., n. 260339.

[156] Cass., Sez. Un., 28 gennaio 2004, *Ferazzi*, in *Cass. pen*., 2004, p. 1913 ss.

[157] Cass., Sez. VI, 6 ottobre 1998, n. 2882, *Calcaterra*, in *C.E.D. Cass.*, 1998, n. 212678. Il provvedimento deve individuare, almeno nelle linee essenziali, gli oggetti da sequestrare con riferimento a specifici fatti di reato, onde evitare che perquisizioni e sequestri si trasformino in mezzi di ricerca della *notitia criminis*.

[158] Cass., Sez. III, 15 gennaio 2016, n. 31415, in *Cass. pen*., 2016; Cass., Sez. IV, 17 novembre 2010, n. 2622, *Rossini,* in *C.E.D. Cass*., n. 249487; Cass., Sez. III, 12 febbraio 2002, *Pedron*, in *Cass. pen*., 2003, p. 970 ss; Cass, Sez. VI, 7 aprile 1997, *Iannini*, in *C.E.D. Cass*., n. 207591.

In relazione alla tutela del segreto[159], può darsi il caso che il *computer* sequestrato o di cui è disposta la copia del disco rigido sia in uso ad un soggetto titolare di un segreto professionale o d'ufficio.

Le garanzie previste in tema di esame testimoniale vengono anticipate, in scala ridotta, nella fase delle indagini preliminari. Ai sensi dell'art. 256 c.p.p., di fronte ad un decreto di esibizione di atti e documenti, ma anche di dati, informazioni e programmi informatici, i soggetti di cui agli artt. 200 e 201 hanno il dovere di consegnarli, «*salvo che dichiarino per iscritto che si tratti di segreti di Stato ovvero di segreto inerente al loro ufficio o professione*». In quest'ultimo caso, l'autorità giudiziaria può procedere comunque agli accertamenti necessari, se ritiene dubbia la fondatezza dell'opposizione e se la mancata acquisizione degli atti non consente di procedere. Dispone il sequestro se la dichiarazione risulta infondata.

Dal mancato rispetto della disciplina su esposta deriva l'illegittimità del provvedimento di sequestro, come rilevato dalla sentenza della Corte di Cassazione, sezione I, *Pomarici*[160]. Nel caso di specie, la realizzazione di una copia *dell'hard disk* del dispositivo in uso ad un giornalista (non indagato), finalizzata a risalire alla fonte della rivelazione di un atto segretato, contrasta con l'art. 256 e con la tutela - non assoluta - apprestata ai giornalisti professionisti dall'art. 200, comma terzo, limitata ai soli nomi delle persone da cui hanno ricevuto notizie di carattere fiduciario[161]. I giudici di legittimità hanno, a rigore, osservato che «*una ricerca senza limiti delle fonti di certe notizie potrebbe rischiare di dare luogo ad un "sostanziale" aggiramento del principio di cui all' art. 200, comma 3, c.p.p.*».

Su questo tema, la Grande Camera della Corte europea dei diritti dell'uomo[162] ha ribadito la necessità di rispettare la disciplina a tutela del segreto giornalistico, in quanto funzionale ad assicurare il diritto alla libertà di espressione, che non ammette

---

[159] Per approfondimenti sul tema, si veda V. NUZZOLESE, *In tema di sequestro di computer ai giornalisti*, in in *Dir. pen. proc*., 2009, n. 3, p. 369; E. APRILE, *Sequestro del computer di un giornalista, clonazione della relativa memoria e tutela del segreto professionale*, in *Dir. Int*. 2007, p. 587.

[160] Cass., Sez. I, 16 febbraio 2007, n. 237430, *Pomarici*, in *Cass. pen*., 2008, p. 2956 ss.

[161] Un'interpretazione in senso restrittivo dell'art. 200, comma terzo, svuoterebbe di contenuto le garanzie previste per i giornalisti professionisti. Dunque, la tutela «*deve ritenersi necessariamente estesa a tutte le indicazioni che possono condurre all'identificazione di coloro che hanno fornito fiduciariamente le notizie*». Cass., Sez. VI, 11 maggio 2004, n. 22397, (udienza 21 gennaio 2004), *Moretti,* Rv 229396.

[162] Corte EDU, Grande Camera, 14 settembre 2010, n. 38224, *Sanoma Uitgevers B.V. c. Paesi Bassi*, in *Cass. pen*., 2011.

deroghe nemmeno dinanzi all'esigenza di accertamento dei reati. Pertanto, il provvedimento dell'autorità giudiziaria di sequestro del materiale posseduto da un giornalista è illegittimo, nella parte in cui pregiudica l'esercizio dell'attività giornalistica, poiché contrasta con il diritto alla libertà di espressione.

3. Il sequestro mediante l'utilizzo di un captatore informatico

Tra le funzioni del captatore informatico compare anche la memorizzazione del contenuto dell'*hard disk* del dispositivo elettronico *target*, con possibilità di copiare, in tutto o in parte, le unità di memoria del sistema informatico.

Com'è evidente, si tratta di un'attività finalizzata a pervenire al medesimo risultato del sequestro informatico sopra menzionato: la clonazione di dati, documenti e programmi informatici, da utilizzare a fini probatori ed analizzabile in ogni momento.

Prima di affrontare le questioni inerenti all'ammissibilità o meno dello strumento, è opportuno tracciare i lineamenti del sequestro mediante captatore, altrimenti definibile "dinamico", e le linee di confine esistenti rispetto agli altri mezzi di ricerca della prova.

Astrattamente, tale tipo di mezzo di ricerca della prova si configura come un sequestro *sui generis*, ancor più 'dematerializzato' rispetto al sequestro informatico "statico", di cui si è discusso in precedenza.

La staticità si lega alla realizzazione di una copia del contenuto di un dispositivo elettronico non utilizzato al momento dell'operazione. Conseguentemente, i dati duplicati sono "fermi" e coincidono con quelli immagazzinati e archiviati nella memoria del disco rigido.

Al contrario, la dinamicità propria del sequestro eseguito mediante captatore informatico si lega alla rapidità e all'istantaneità della copia informatica "*online*", potenzialmente realizzabile anche su dati *in fieri*, essendo in tempo reale.

Il captatore agisce in tal caso da "copiatore informatico"[163], rientrando, a quanto pare, nell'attività di *online search*[164]. Dalla "sorveglianza" *online* del sistema elettronico *target* alla clonazione digitale del suo contenuto, il passo è breve.

Il sequestro dinamico si distingue dalla perquisizione effettuata con le medesime modalità. Il primo si traduce in un'acquisizione dei dati, la seconda, invece, si limita ad un'attività di ricerca probatoria. Tuttavia, si registra una tendenza ad assimilare le due fasi da parte della dottrina e della giurisprudenza che finora sono venute a contatto con questa delicata materia.

Il caso *Virruso*, di cui si è precedentemente dato conto (cfr. cap. III), ne è un esempio. Il decreto del pubblico ministero, peraltro ritenuto bastevole a giustificare l'intrusione informatica, si riferisce, indifferentemente, al prelevamento e alla copia dei documenti memorizzati nel disco rigido.

Ma, non può essere realizzata per via interpretativa una confusione dei mezzi di ricerca della prova, i cui tratti essenziali e finalità sono state cristallizzati dal legislatore nel testo normativo.

Bisogna ammettere che manca una definizione esatta del contenuto degli stessi, in previsione di un necessario adattamento alle modalità e agli strumenti che il progresso è in grado di offrire. Ma, anche quando la realtà su cui ricade l'attività investigativa perde materialità e contingenza, il punto fermo per l'interprete resta il dettato normativo. Si ritiene, quindi, preferibile mantenere la tradizionale distinzione e concatenazione tra ispezioni, perquisizioni e sequestri. In relazione al dato digitale, acquisito sia in maniera "statica", sia "dinamica", si propone sinteticamente la seguente ricostruzione dell'attività di ricerca della prova digitale.

Le ispezioni si limitano all'osservazione esterna del sistema mediante la descrizione del suo *status*, degli eventuali *software* attivi, nonché delle periferiche e delle connessioni[165]. Ma, «*se è vero che la percezione sensoriale dovrebbe prescindere, in tale contesto, anche da semplici forme di interazione con il sistema informatico sottoposto a*

---

[163] M. TROGU, *Sorveglianza e "perquisizione" online su materiale informatico*, cit., pp. 442 e 445. Si riprende quella distinzione tra "copiatore informatico" e "appostamento informatico", di cui al cap. I, § 2.

[164] Cfr. cap. I, § 2.

[165] M. PITTIRUTI, *Profili processuali della prova informatica*, in L. MARAFIOTI – G. PAOLOZZI (a cura di), *'Incontri ravvicinati' con la prova penale. Un anno di seminari a Roma Tre*, Torino, 2014, pp. 55-56.

verifica»[166], non si spiega la ragione del richiamo all'adozione di misure tecniche dirette ad assicurare la conservazione dei dati digitali e ad impedirne l'alterazione. Sembra, quindi, possibile ammettere anche una forma di ispezione successiva all'ingresso nel sistema informatico (una sorta di ispezione digitale nella perquisizione informatica), avente ad oggetto la constatazione dell'esistenza di un certo documento o programma informatico, avente una certa denominazione e con determinate proprietà. Solo la perquisizione consente l'ingresso nel sistema informatico o telematico e l'eventuale apertura dei documenti oggetto d'interesse investigativo.

Infine, s'intende aderire alla tesi per cui «*ogni operazione di prelevamento del dato non acconsentita dal suo titolare va appunto intesa come sequestro*»[167]. Il decreto di autorizzazione dovrebbe dare conto di tale differenziazione, altrimenti lo stesso interessato non viene posto nelle condizioni di poter avere contezza del diverso grado di intrusione digitale.

4. Circa l'ammissibilità di un sequestro informatico mediante captatore

Passando ora più specificamente ad affrontare il tema dell'eventuale legittimità del sequestro a distanza mediante virus informatico, la natura e le modalità dello strumento captativo sembrano ostare ad una risposta positiva.

Come in tema di ispezioni e di perquisizioni, manca una disciplina specifica in materia. In relazione al sequestro del dato digitale, la più volte citata legge n. 48 del 2008 si è limitata ad estendere espressamente l'art. 254 c.p.p., che prevede il sequestro di corrispondenza, anche a quella inoltrata per via telematica, considerata alla stregua di una lettera in busta chiusa.

L'art. 8, comma quinto, della stessa legge n. 48 del 2008 ha interpolato nell'ordito del c.p.p. un nuovo art. 254-*bis*, nel quale si è prevista una ipotesi di sequestro

[166] E. M. MANCUSO *L'acquisizione dei contenuti e-mail*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, p. 73.
[167] G. SCHENA, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, cit., p. 302.

avente ad oggetto i dati conservati presso i fornitori di servizi informatici, telematici e di telecomunicazioni, che può avvenire mediante copia di essi su adeguato supporto, al fine di garantire la continuità nella fornitura dei servizi medesimi.

L'art. 19 della Convenzione di Budapest, a sua volta, richiedeva alle parti contraenti di introdurre una previsione normativa che consentisse all'autorità procedente di «*sequestrare o acquisire in modo simile i dati informatici per i quali si è proceduto all' accesso*» o perquisizione[168]. L'innovatività della riforma risulta, pertanto, piuttosto contenuta.

Però, per quanto la formula "*acquisire in modo simile*" sia piuttosto ampia, non sembra trovare spazio né nella Convezione sulla criminalità informatica, né nella legge che alla stessa ha dato attuazione, n. 48 del 2008, una forma occulta e a distanza di acquisizione dinamica dei dati, quale quella ottenibile mediante l'utilizzo di un virus informatico.

Né sembra possibile una applicazione analogica delle disposizioni vigenti in materia di sequestro informatico, sopra richiamate.

Infatti, l'art. 253, comma quarto, prescrive la consegna della copia del decreto motivato all'interessato, se presente[169], con funzione garantistica preventiva e successiva: in via preliminare, mira a scongiurare sequestri arbitrari, del tutto sganciati dalla sussistenza dei presupposti normativi. Successivamente, consente all'interessato di verificare la fondatezza e la legittimità dell'operazione, che può essere messa in dubbio attraverso il riesame[170], anche nel merito, a norma dell'art. 324.

---

[168] Le misure da introdurre «*devono includere il potere di: a. sequestrare o acquisire in modo simile un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici; b. fare e trattenere una copia di quei dati informatici; c. mantenere l'integrità dei relativi dati informatici immagazzinati; d. rendere inaccessibile o rimuovere quei dati dal sistema informatico analizzato*».

[169] Nello stesso senso, al termine delle operazioni, «*in ogni caso la persona o l'ufficio presso cui fu eseguito il sequestro ha diritto di avere copia del verbale dell'avvenuto sequestro*» *ex* art. 258, comma terzo.

[170] Si osservi che l'interessato può far valere, *ex multis*, l'esuberanza del vincolo di sequestro rispetto al legame pertinenziale dei beni con il reato contestato. In relazione al dato digitale, è frequente l'ipotesi di un sequestro che supera i limiti segnati dal collegamento dei beni al reato e dalla finalità del provvedimento. Cass., Sez. V, 18 marzo 2004, n. 22818, in *C.E.D. Cass.*, 2004, n. 228818. Inoltre, il Tribunale del riesame può annullare il decreto di sequestro se l'indeterminatezza della contestazione non consente l'individuazione del *fumus commissi delicti* e la sussunzione della fattispecie in quella prevista dalla legge. Cass., Sez. II, 12 dicembre 2008, n. 47617, *De Luigi*, in *C.E.D. Cass.,* 2008, n. 242304. Tuttavia, può ritenere la sussistenza del *fumus* in relazione ad una diversa qualificazione giuridica del medesimo fatto storico. Cass., Sez. V, 18 novembre 2004, n. 49376, in *C.E.D. Cass*., 2005, n. 230428.

Invece, l'installazione del *virus* informatico destinato alla apprensione dei dati contenuti nel dispositivo *target,* onde realizzare un sequestro "dinamico" ed a distanza, avviene furtivamente, sfuggendo all'attenzione dell'interessato. Quest'ultimo non verrà a conoscenza dell'avvenuta intrusione da parte degli organi inquirenti. Ne conseguirebbe, inevitabilmente, la mancata attivazione incolpevole dei meccanismi di tutela previsti dalla legge.

Verrebbe meno quel naturale contatto diretto con l'autorità giudiziaria che la consegna del decreto presuppone e che il legislatore prevede implicitamente (si pensi alla disciplina prevista a tutela dei segreti). Ma vi è di più. L'interessato verrebbe di fatto privato del diritto ad impugnare il provvedimento e del diritto alla restituzione delle cose sequestrate.

In sostanza, la clonazione occulta dei dati contenuti nel sistema informatico attenzionato realizzerebbe un vero e proprio aggiramento delle garanzie individuali previste dalla legge, a tutela del diritto di difesa, del principio del contraddittorio, nonché del segreto epistolare.

Si consideri, inoltre, che laddove si tratti di un sequestro di corrispondenza avente ad oggetto dati inoltrati per via telematica o detenuti da fornitori di servizi informatici, telematici o di telecomunicazioni, l'interessato non avrebbe alcuna certezza della mancata apertura o alterazione del contenuto degli stessi. A tal proposito, l'art. 254, comma terzo, vieta agli ufficiali di polizia giudiziaria di prendere conoscenza del contenuto della corrispondenza sequestrata, costituente una *species* del *genus* comunicazione. Parimenti, in relazione all'art. 254-*bis*, l'art. 132 del d.lgs. 30 giugno 2003, n. 196, esclude «*i contenuti di comunicazione*» del traffico telefonico o telematico dagli obblighi di conservazione per gli operatori dei servizi di telecomunicazione.

Inoltre, l'ignoranza da parte del soggetto *target* della acquisizione in copia dei dati non può conciliarsi con il rispetto della disciplina dettata a tutela del segreto professionale, d'ufficio e di Stato. I soggetti di cui agli artt. 200 e 201 possono essere esonerati dal dovere di esibizione di quanto richiesto da parte dell'autorità giudiziaria, se la dichiarazione in forma scritta che attesti la segretezza del dato richiesto risulti fondata e la prosecuzione delle indagini non è inibita dalla mancata acquisizione degli atti.

Per quanto non si possa negare un'ampia discrezionalità degli organi inquirenti, la previsione di una tutela legislativa dei segreti non può essere posta nel nulla attraverso

l'introduzione surrettizia di strumenti non previsti dalla legge, che non consentono di sollevare tale eccezione.

In chiave ancor più garantistica, in ragione della natura del segreto, l'art. 256-*ter*, di fronte all'eccezione opposta dal responsabile dell'ufficio circa la sussistenza di un segreto di Stato, prevede la sospensione dell'esame o della consegna dell'atto o della cosa. Il Presidente del Consiglio dei Ministri, a cui viene trasmesso l'oggetto di interesse sigillato, può confermare l'esistenza del segreto entro trenta giorni ed evitarne così l'acquisizione.

Alla luce delle osservazioni su esposte, sembra potersi affermare che l'acquisizione *online* dei dati contenuti all'interno del disco rigido, attuata in modalità volutamente nascosta, sia, ancor prima che illegittima, incostituzionale.

In relazione all'art. 111, comma terzo, Cost., non è garantito il diritto della persona accusata di un reato ad essere informata, in maniera tempestiva e riservata, della natura e dei motivi dell'accusa elevata a suo carico. Ma, sembra profilarsi una violazione ancor maggiore. Che l'indagato o l'imputato, non venga edotto del motivo, in fatto e in diritto, posto alla base di un atto autoritativo lesivo della sua sfera privata, non costituisce la preoccupazione principale dell'interprete, se la si rapporta ad un'ulteriore circostanza.

La massima gravità della violazione viene raggiunta in un momento antecedente, individuato nel compimento dell'atto invasivo in maniera occulta, in spregio dei diritti fondamentali dell'uomo e dei principi di una società democratica.

La prova che per tale via verrebbe a formarsi sarebbe, senza dubbio, incostituzionale.

Occorre, infine, considerare che anche nel panorama europeo non può trovare diritto di cittadinanza un'operazione consimile.

L'art. 6, comma terzo, lett. a), assicura ad ogni accusato il diritto di «*essere informato, nel più breve tempo possibile, in una lingua a lui comprensibile e in modo dettagliato, della natura e dei motivi dell'accusa formulata a suo carico*»[171]. Che il termine "*persona accusata*" s'intenda comprensiva anche dell'indagato trova conferma nell'interpretazione della Corte Europea dei diritti dell'uomo, secondo cui la comunicazione dell'addebito deve avvenire sin dalla sua formulazione provvisoria.

[171] L'art. 6 CEDU, rispetto all'art. 111 Cost., contiene due elementi aggiuntivi: il soggetto deve essere informato in una lingua a lui comprensibile e dettagliatamente. L'art. 111, a sua volta, menziona il diritto ad essere informato in forma riservata, profilo assente nella norma europea.

Tale considerazione vale altresì in relazione alla norma costituzionale interna. Per quanto l'art. 111 si riferisca al "*processo penale*" e alla "*persona accusata*", la garanzia informativa va estesa anche, e principalmente, alla fase delle indagini preliminari. Sarebbe, infatti, svuotata di contenuto se la si ritenesse applicabile soltanto nella fase processuale, quando il soggetto viene necessariamente posto nelle condizioni di conoscere l'accusa a suo carico con la formulazione dell'imputazione e la citazione in giudizio.

Nella fase delle indagini preliminari, tale funzione conoscitiva è svolta proprio dalla consegna del decreto motivato con cui si dispone il sequestro ovvero la perquisizione. La giurisprudenza[172] ritiene tale atto equipollente all'informazione di garanzia, purché ne contenga gli elementi essenziali e l'interessato sia presente e sia stato posto nelle condizioni di esercitare il suo diritto di difesa, mediante l'assistenza di un difensore[173]. L'assenza dell'indagato comporta, invece, la riemersione dell'obbligo del pubblico ministero di tempestivo inoltro dell'informazione di garanzia, dopo il compimento dell'operazione, poiché viene meno l'esigenza preclusiva connessa alla natura di atto a "sorpresa"[174].

---

[172] G. CONSO– V. GREVI - M. BARGIS, *Compendio di procedura penale*, cit., p. 525. Cass., Sez. Un., 23 febbraio 2000, *Mariano*, in *Diritto e giustizia* 2000, n. 22, p. 18. In senso conforme, Cass., Sez. V, 15 giugno 2000, *Madonia*, in *Cass. pen*. 2002, p. 2385; Cass., Sez. III, 7 novembre 2002, *Agliolo,* in *C.E.D. Cass*., n. 223377-223376. Trib. Milano, 18 gennaio 2001, in *Foro ambrosiano*, 2002, p. 479. Il decreto di sequestro contiene in sé l'informazione di garanzia, se dispone l'avviso all'indagato che il pubblico ministero procede nei suoi confronti in relazione a determinati reati. Cass., Sez. III, 19 febbraio 2014, n. 22898, in *Diritto e giustizia,* 2014.

[173] In dottrina, sulla contestualità dell'informazione di garanzia rispetto al compimento dell'atto a sorpresa per cui è richiesta, si veda F. CORDERO, *Procedura penale*, II ed., Giuffré, 1993, p. 752; G. TRANCHINA in D. SIRACUSANO – A. GALATI – G. TRANCHINA – E. ZAPPALA, *Diritto processuale penale*, II ed., Giuffré, 1996, vol. II, p. 147.

[174] P. FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 282. «*In termini analoghi si dovrebbe ritenere necessario l'inoltro dell'informazione subito dopo il compimento della perquisizione quando questa si debba eseguire presso persona diversa da quella sottoposta alle indagini*».

5. La captazione della posta elettronica e delle *e-mail* in "bozza" mediante *virus* informatico

La posta elettronica o informatica consente l'invio e la ricezione di dati, documenti, contatti attraverso un sistema informatico. Tecnicamente, il messaggio passa da *server* in *server* sino ad arrivare al *server* del destinatario grazie al c.d. *Mail Transport Agent* (MTA)[175].

Non si richiede una contestuale connessione degli interlocutori, poiché la modalità di accesso al servizio è asincrona[176]. La comunicazione ha inizio con il messaggio registrato nella memoria gestita dal mittente, trasferito al destinatario grazie al fornitore del servizio – il c.d. *e-mail provider* -, «*in attesa che l'utente interessato si colleghi alla sua casella postale* (c.d. *account*)». A questo punto, il messaggio viene «'*scaricato' dal destinatario sulla memoria del proprio computer, e qui registrato*»[177] per la lettura.

Oltre a questa modalità di accesso[178], che si avvale di programmi *client* di posta, è possibile anche l'accesso da remoto attraverso la rete (la c.d. *web mail*).

La portabilità del dato digitale implica la sua 'scorporabilità' dal supporto che lo contiene: il contenuto della lettera elettronica può essere trasferito «*una serie infinita di*

---

[175] Il *server* MTA del destinatario consegna il messaggio al *server* di posta elettronica in entrata, definito *Mail Delivery Agent* (MDA), che lo immagazzina in attesa che l'utente venga a rilevarlo. L'accesso all'MDA è protetto da un nome utente e da una *password*, attraverso i quali si effettua il c.d. "*login*".
I principali protocolli che consentono di rilevare la posta su un MDA sono *Post Office Protocol* (POP3), il meno aggiornato, e *Internet Message Access Protocol* (IMAP), che conserva sempre una copia del messaggio sul *server* al fine di assicurare la sincronizzazione dello stato dei messaggi (cancellato, letto, spostato) tra più *client* di posta elettronica (*Microsoft Outlook*, *Microsoft Mail*, *Apple Mail*, ad esempio). Quando, invece, l'accesso avviene da remoto mediante un'interfaccia *web*, il contenuto della posta elettronica viene consultato in rete, la c.d. *web mail* o *web access*.

[176] A. MACRILLÒ, *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. Int*., 2008, p. 513.

[177] La presente citazione, unita a quella precedente, sono tratte da una ricostruzione ideale delle diverse fasi in cui si articola la trasmissione del messaggio, realizzata da C. PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, p. 294.

[178] G. SCHENA, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, in *Cass. pen.* 2016, n. 1, p. 306. «*Il discorso è di attuale interesse poiché a seconda delle modalità di accesso alla posta elettronica mutano anche le modalità del sequestro. A parità di condizioni normative, la scelta più garantista sembrerebbe l'accesso tramite service provider e account*». Si veda anche A. LOGLI, *Sequestro probatorio di un personal computer*. *Misure ad explorandum e tutela della corrispondenza elettronica,* cit., p. 2958.

volte, senza differenze qualitative dall'originale»[179]. In altri termini, gli elementi di prova di natura digitale cambiano il contenitore, ma conservano il contenuto.

In ogni caso, l'*e-mail* presenta un contenuto comunicativo ed intersubiettivo[180].

L'apprensione della corrispondenza elettronica[181] costituisce il crocevia di diversi istituti giuridici. L'acquisizione della stessa all'interno del processo penale segue regole diverse a seconda della "fase" in cui si trova il messaggio e delle modalità operative adottate dagli organi inquirenti.

Tra le forme di possibile acquisizione, si segnala la captazione in tempo reale anche mediante l'impiego di un captatore informatico con invio immediato o ad intervalli prestabiliti di una copia delle *e-mail* al *server* della Procura procedente.

La qualificazione giuridica di tale attività non è immediatamente individuabile. Esiste, infatti, una labile linea di demarcazione tra la disciplina delle intercettazioni informatiche e quella relativa ai sequestri.

Secondo un criterio di tipo funzionale[182], occorre distingue tra attività occulta e palese[183]. Nel primo caso, la captazione avviene all'insaputa del destinatario e richiede l'applicazione della disciplina più garantita delle intercettazioni informatiche o telematiche; nel secondo caso, invece, l'atto, per quanto a "sorpresa", è scoperto e garantito. L'acquisizione dei dati si traduce, quindi, in un'attività di sequestro.

---

[179] F. ZACCHÈ, *La prova documentale*, G. UBERTIS – G. P. VOENA (diretto da), *Trattato di procedura penale*, Milano, XIX, 2012, p. 35. L'A. sottolinea la differenza con il documento tradizionale, in cui «*la rappresentazione è incorporata in modo inscindibile nella res che memorizza e conserva*», così che «*ogni copia sarà sempre qualcosa d'altro rispetto all'originale*».

[180] P. BARILE – E. CHELI, *Corrispondenza [libertà di]*, *Enc. dir*., X, Milano, 1962, p. 744. Non rilevano né il mezzo di trasmissione, né la forma. È sufficiente che «*l'espressione dell'idea o della notizia, per acquisire il carattere di comunicazione, dev'essere formulata da un soggetto, (mittente) al fine di farla pervenire nella sfera di conoscenza di uno o più soggetti determinati (destinatari)*».

[181] Ai sensi dell'art. 616 c.p., seppur limitatamente agli effetti delle disposizioni della sezione V (*Dei delitti contro l'inviolabilità dei segreti*), «*per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza*».

[182] Un limite significativo di tale criterio è costituito dalla rimessione della scelta della disciplina applicabile all'arbitrio degli organi inquirenti, a cui è rimessa la valutazione circa la convenienza di agire in incognito ovvero di optare per un'operazione palese. Oltre al criterio funzionale, si segnalano almeno altri due criteri. In primo luogo, il criterio temporale, secondo cui la contestualità tra la captazione e la trasmissione dell'*e-mail* implica il ricorso all'intercettazione telematica, avente ad oggetto dati "*in itinere*". In caso contrario, si applica la disciplina dei sequestri. In secondo luogo, è stato di recente introdotto il criterio dell'inoltro. Si veda, a tal proposito, Cass., Sez. IV, 28 giugno 2016, in *C.E.D. Cass*., n. 268228.

[183] F. ZACCHÈ, *L'acquisizione della posta elettronica nel processo penale*, cit., p. 109. G. VACIAGO, *Digital evidence. I mezzi di ricerca della prova digitale e le garanzie dell'indagato*, Torino, 2012, p. 81.

In realtà, come dimostra il caso "*Virruso*" (cfr. Cap. III, § 7), il *virus* informatico è perfettamente in grado di realizzare un'acquisizione occulta dei dati contenuti nel dispositivo elettronico attenzionato, agendo in incognito.

In entrambi i casi, e a prescindere dalla disciplina applicabile, la costante è costituita dal carattere occulto dell'attività investigativa posta in essere.

Se l'oggetto della captazione è costituito da un flusso[184] bidirezionale di dati a carattere comunicativo, che passa all'interno di un sistema informatico o telematico ovvero che intercorre tra più sistemi informatici o telematici, la disciplina applicabile va individuata nell'art. 266-*bis*[185].

In tal caso, la captazione della posta elettronica mediante l'utilizzo di un captatore informatico è ammissibile, come espresso dalla sezione V della Corte di Cassazione nella sentenza *Occhionero* (cfr. Cap. II, § 9).

L'apprensione della comunicazione è contestuale alla sua trasmissione. Pertanto, non vi sono dubbi circa l'attualità della stessa.

Ne consegue l'applicazione della tutela rafforzata di cui all'art. 15 Cost., a protezione della libertà e della segretezza della corrispondenza.

La riserva di giurisdizione è integrata dall'autorizzazione del giudice per le indagini preliminari. In proposito, si segnala l'orientamento secondo cui non costituisce causa di invalidità o di inutilizzabilità del provvedimento la mancata individuazione sia dell'*account* di posta elettronica sia di quello di connessione[186]. Trattandosi di due aspetti della medesima realtà giuridica, indicativa della facoltà di accesso di un determinato nome utente alla trasmissione e alla ricezione dei flussi telematici, può essere sufficiente l'individuazione dell'utilizzatore mediante la sola specificazione dell'*account* di posta elettronica[187].

---

184 Cass., Sez. IV, 28 giugno 2016, n. 40903, *Grassi ed altri*, in *C.E.D. Cass*., n. 268228. «*Il "flusso" consiste nello scambio di dati numerici (bit). Oggetto di intercettazione informatica o telematica è la connessione, fissa o occasionale, tra computer tra loro collegati o in rete o via modem o con qualsiasi altra forma*».

185 Sull'applicazione estensiva della disciplina più garantista di cui all'art. 266-*bis*, si veda E. M. MANCUSO *L'acquisizione dei contenuti e-mail*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, p. 69. Secondo l'A., alla consegna del messaggio, l'allocazione, seppur temporanea, dello stesso presso il *service provider* del destinatario implica in ogni caso l'instaurazione di un successivo «*flusso tra sistemi informatici – id est, tra il server appena menzionato e il terminale remoto che utilizza i programmi di lettura della posta - che consente al beneficiario di ottenere una copia del messaggio*».

186 Cass., Sez. I, 6 febbraio 2005, *Palamara*, in *C.E.D. Cass.,* n. 231591. Si veda anche Cass., Sez. IV, 9 novembre 2005, n. 4213. *Contra*, M. TROGU, *Le intercettazioni di comunicazioni a mezzo Skype*, in *Processo penale e Giustizia*, 2014, n. 3, p. 104.

187 *Contra*, M. TROGU*, Le intercettazioni di comunicazioni a mezzo Skype*, cit., p. 104.

Meno garantita è, invece, la disciplina applicabile nel caso in cui venga disposta con il solo decreto del pubblico ministero la clonazione occulta del contenuto del disco rigido, contenente, com'è ovvio, anche la corrispondenza elettronica.

Precedentemente all'intervento della legge n. 48 del 2008, una parte della dottrina riteneva applicabile la disciplina di cui all'art. 266-*bis* per captare la lettera elettronica non ancora letta dal destinatario[188], anche se allocata presso il gestore del servizio. Successivamente alla lettura del messaggio, gli istituti giuridici di riferimento andrebbero individuati nella perquisizione e nel sequestro.

L'aggiunta dell'art. 254-*bis* e la modifica dell'art. 254, in modo da consentire il sequestro di corrispondenza inoltrata per via telematica presso i fornitori di servizi telematici o di telecomunicazioni, sembrano aver normativamente risolto la questione a favore dell'applicazione della normativa in tema di sequestri.

Tuttavia, restano comunque parzialmente irrisolte le questioni interpretative inerenti alla non sempre agevole distinzione tra la captazione occulta e dinamica di un flusso di comunicazioni in corso di svolgimento, autorizzata dal g.i.p., e il sequestro di corrispondenza elettronica, disposta dal pubblico ministero con decreto consegnato all'interessato, se presente.

Il primo criterio discretivo proposto si lega ai rapporti temporali intercorrenti tra il momento in cui avviene la captazione e quello in cui si realizza la trasmissione dell'*e-mail*. La contestualità delle due operazioni implica il ricorso all'intercettazione telematica[189], avente ad oggetto dati "*in itinere*". In caso contrario, si applica la disciplina dei sequestri.

Parte della dottrina ha, tuttavia, sottolineato l'inadeguatezza di tale distinzione nei casi *"border line*" in cui si verifichi un «*ritardo nella consegna del messaggio dal server del mittente a quello del destinatario*» ovvero nell'ipotesi in cui venga acquisita «*un'e-mail in transito sul server del gestore, quando la polizia procede al sequestro della posta*

[188] R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 135.

[189] E. APRILE, Intercettazioni di comunicazioni, in A. SCALFATI (a cura di), *Prove e misure cautelari*, in *Trattato di procedura penale*, diretto da G. SPANGHER, vol. II, tomo I, Torino, 2009, p. 535.

ivi archiviata», o, ancora, in caso di un'*e-mail* 'scaricata' sul dispositivo del destinatario, ma non letta[190].

È stato altresì osservato che alla consegna del messaggio, l'allocazione, seppur temporanea, dello stesso presso il *service provider* del destinatario implica in ogni caso l'instaurazione di un successivo «*flusso tra sistemi informatici – id est, tra il server appena menzionato e il terminale remoto che utilizza i programmi di lettura della posta - che consente al beneficiario di ottenere una copia del messaggio*»[191]. Ne consegue l'opportunità di propendere a favore della soluzione più garantista di cui all'art. 266-*bis*.

Si è proposto, inoltre, un secondo criterio, di tipo funzionale, che distingue tra attività occulta e palese[192]. Nel primo caso, la captazione avviene all'insaputa del destinatario e richiede l'applicazione della disciplina più garantita delle intercettazioni informatiche o telematiche; nel secondo caso, invece, l'atto, per quanto a "sorpresa", è scoperto e garantito. L'autorità procedente accede al gestore del servizio o al dispositivo dell'interessato in maniera necessariamente palese. L'acquisizione dei dati si traduce, quindi, in un'attività di sequestro.

In realtà, entrambi i criteri risultano inappaganti. Il primo non sembra tenere in debito conto la relatività del concetto di attualità e contestualità della comunicazione elettronica, che emerge se si considera che il destinatario può prendere visione anche dopo diversi giorni del contenuto del messaggio. Nondimeno, il criterio funzionale subordina la scelta della disciplina applicabile all'arbitrio degli organi inquirenti, a cui è rimessa la valutazione circa la convenienza di agire in incognito, dietro autorizzazione del giudice, ovvero di optare per un'operazione palese, seguendo le regole in tema di sequestri.

Un particolare utilizzo del captatore informatico finalizzato ad apprendere la corrispondenza elettronica intercorrente tra gli indagati, si rinviene in una recente decisione della Corte di Cassazione (Sezione IV, 28 giugno 2016, *Grassi ed altri*).

Le indagini miravano allo smascheramento di un'organizzazione criminale dedita al traffico di stupefacenti di provenienza estera.

---

190 Cfr. F. ZACCHÈ, *L'acquisizione della posta elettronica nel processo penale*, cit., p. 109.

191 E. M. MANCUSO *L'acquisizione dei contenuti e-mail*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, p. 69.

192 F. ZACCHÈ, *L'acquisizione della posta elettronica nel processo penale*, cit., p. 109. G. VACIAGO, *Digital evidence. I mezzi di ricerca della prova digitale e le garanzie dell'indagato*, Torino, 2012, p. 81.

Il ricorso da parte degli imputati ad una peculiare tecnica comunicativa, le *e-mail* in "bozza", ha reso possibile l'apprensione delle stesse, non inoltrate, direttamente attraverso l'accesso all'*account* di posta elettronica da loro utilizzato.

A tal fine, gli inquirenti hanno installato un captatore informatico all'interno del computer ubicato presso un Internet Point, con attivazione della funzione *keylogger*, così da carpire le *password* d'accesso digitate sulla tastiera.

In relazione alla captazione delle *e-mail* spedite o ricevute, i giudici di legittimità hanno ritenuto applicabile l'art. 266-*bis*, la cui introduzione nel 1993 mirava ad estendere la tutela a tutti i dati informatici in transito nel sistema di riferimento, compresi quelli non integranti una «*conversazione tra persone, nei sensi di cui all'art. 266*», «*relativi al traffico dei servizi complementari, - alla telefonia mobile -, quali il servizio "messaggi" (es. tipo E-MAIL, o Fax)*»[193].

Dunque, non rileva la mancanza di attualità del flusso di dati ai fini dell'applicazione della disciplina delle intercettazioni anche nelle ipotesi in cui l'apprensione non sia contestuale alla comunicazione. Il principio non presenta profili di particolare novità, in quanto già affermato in relazione all'acquisizione di messaggi mediante il sistema "*pin to pin*"[194] tra dispositivi *Blackberry*[195].

Secondo quanto ritenuto dai giudici di legittimità, il criterio discretivo tra l'applicazione della disciplina delle intercettazioni e quella relativa ai sequestri va individuato non nel criterio temporale, bensì nel criterio dell'inoltro[196].

La proposta, tuttavia, non convince. La disciplina del sequestro, introdotta con la l. 48 del 2008, verrebbe così relegata ai marginali casi in cui l'*e-mail* non è inviata, ma "parcheggiata" in bozza, all'illecito scopo di sfuggire alle investigazioni, come è avvenuto nel caso di specie.

---

193 Cass., Sez. Un., 13 luglio 1998, n. 21, *Gallieri*, in *C.E.D. Cass.*, n. 211117.

194 Il PIN è un codice univoco identificativo proprio dei dispositivi *Blackberry*, simile al codice IMEI.

195 Cass., Sez. III, 10 novembre 2015, n. 50452, *Guarnera ed altri*, in C.E.D. Cass., n. 265615; Cass., Sez. III, 9 marzo 2016, n. 17193, *Calabrò,* non mass.

196 Cass., Sez. IV, 28 giugno 2016, n. 40903, *Grassi ed altri*, in *C.E.D. Cass*., n. 268228. «*Il discrimine perché ci sia stato o meno "flusso informatico" - e quindi debba essere applicata la disciplina delle intercettazioni e non quella del sequestro- è nell'avvenuto inoltro dell'e-mail da parte del mittente. Perciò, ritiene il Collegio che, quanto alle e-mail inviate o ricevute la risposta da fornire al quesito circa l'esistenza o meno di un flusso informatico sia positiva*».

Se da un lato si valorizza la l. 547 del 1993, dall'altro si svuota di contenuto una legge per di più successiva, che, per quanto non possa definirsi una svolta epocale, in ogni caso merita apprezzamento.

Corollario del ragionamento della Corte sembra essere l'acquisizione dei contenuti salvati in bozza attraverso la disciplina del sequestro di dati informatici[197], che non necessita di un'autorizzazione del giudice.

Le *e-mail* in bozza realizzano un sistema comunicativo differito, che non rientrerebbe nella nozione di corrispondenza. Sul punto, si consenta di dissentire.

A prescindere dalla disciplina applicabile, non può negarsi che un sistema di scambi informativi così congegnato possa integrare una corrispondenza e, in ogni caso, rientra senza dubbio nel concetto di comunicazione.

Se è vero, com'è vero, che non costituisce «*corrispondenza o comunicazione un qualsiasi scritto, anche se redatto in forma epistolare, destinato a rimanere come appunto, nota, diario personale*», occorre considerare - com'è stato autorevolmente considerato - che «*esso diverrà corrispondenza soltanto quando il soggetto che lo ha redatto maturi l'intenzione di farlo pervenire ad un altro soggetto*»[198].

Pertanto, poiché l'art. 15 Cost. tutela la corrispondenza ed «*ogni altra forma di comunicazione*», nel caso di specie, l'assunto per cui viene ritenuto bastevole il decreto del pubblico ministero mal si concilia con la doppia riserva di legge e di giurisdizione.

Tuttavia, come sottolinea la stessa Corte in relazione alle *e-mail* spedite e/o ricevute, l'esistenza di un provvedimento autorizzativo del g.i.p., «"*copriva" in termini di garanzie anche tale acquisizione*»[199].

La sentenza in esame presenta diversi profili di interesse e offre numerosi spunti critici.

In relazione alle *e-mail* in bozza, secondo la difesa, il detentore dei dati va identificato nel gestore del servizio, ubicato all'estero[200]. Di qui la necessità di applicare

---

[197] *Contra*, S. DE FLAMMINEIS, *Le intercettazioni telematiche*, in *Dir. pen. proc*., 2013, p. 992. Secondo l'A. le *e-mail* archiviate, anche mediante salvataggio in bozza, «*in un account accessibile anche da altro utente, anche se non si tratta di una e-mail inoltrata al destinatario, sarebbe possibile l'intercettazione del secondo utente al momento dell'accesso alla casella; anche questa quindi deve intendersi come una comunicazione nonostante l'e-mail non sia stata inviata*».

[198] Per questa citazione e per quella precedente, cfr. BARILE P. – CHELI E., *Corrispondenza [libertà di]*, *Enc. dir*., X, Milano, 1962, p. 745.

[199] Cass., Sez. IV, 28 giugno 2016, n. 40903, *Grassi ed altri*, cit., p. 40.

[200] Per i giudici il ricorso ad un *server* straniero non basta per sottrarsi alla giurisdizione italiana.

l'art. 254-*bis*. Invece, secondo il Collegio, i dati restano nella disponibilità dell'utente, perché non inoltrati[201].

Conseguentemente, non solo non si seguono le regole di cui all'art. 254-*bis*, ma nemmeno quelle previste dall'art. 254, data l'assenza di un inoltro e, ancor prima, di una corrispondenza.

A tal proposito, la Corte sembra fare un passo indietro. Pur affermando che «*non vi siano dubbi che per tali e-mail si sia in presenza di un'attività che ricorda quella del sequestro di dati informatici*», non ritiene applicabile né l'art. 254-*bis*, né l'art. 254.
Ma, onde garantire la tenuta del sistema, si afferma quanto segue: «*la violazione delle formalità previste dalle disposizioni richiamate non potrebbe comunque in nessun caso comportare la inutilizzabilità dei risultati della perquisizione o del sequestro in quanto non si tratterebbe di "prove acquisite in violazione di un divieto di legge" (ex art. 191 cod. proc. pen.) ma eventualmente di prove acquisite senza il rispetto delle formalità previste per la loro acquisizione*».

Concentrando l'attenzione sugli aspetti legati all'impiego del captatore informatico, la Corte dà per assunta l'ammissibilità dello strumento, senza soffermarsi sui rischi di lesione dei diritti fondamentali.

Incidentalmente, si afferma che nel caso di specie il programma informatico è stato utilizzato al fine di acquisire le credenziali d'accesso alla casella di posta[202], «*come si è da sempre usata la microspia per le intercettazioni telefoniche o ambientali*»; «*indipendentemente dal sistema di intrusione utilizzato (quello dell'accesso diretto al*

---

[201] Per un'attenta analisi del meccanismo di funzionamento, cfr. A. LOGLI, *Sequestro probatorio di un personal computer*. *Misure ad explorandum e tutela della corrispondenza elettronica,* cit., p. 2958. Se si accede "in remoto" «*i messaggi rimangono archiviati sulla memoria del provider che fornisce la casella di posta elettronica*». Se si utilizzano, invece, programmi di gestione della posta (*outlook*, *mai*l, ecc.) i messaggi «*vengono immediatamente ritrasmessi sul personal computer del destinatario e di essi (almeno che non vengano impostati particolari meccanismi di memorizzazione) non rimane traccia sul computer remoto*». In tal caso, nella memoria del gestore rimarranno solo i dati esterni della comunicazione, acquisibili con le stesse modalità previste per i tabulati telefonici.

[202] L. GIORDANO, *L'uso di captatori informatici nelle indagini di criminalità organizzata*, in *Cass. pen*., 2017, suppl. n. 5, p. 214. L'intrusione informatica nel dispositivo bersaglio «*trova la sua giustificazione nello stesso provvedimento del g.i.p. che ha disposto l'intercettazione ex art. 266-bis all'esito di una ponderazione dei diritti in conflitto tra di loro, consistendo, in ultima istanza, in una modalità attuativa del mezzo di ricerca della prova*».

computer ovvero occulto attraverso un programma spia), quando si vanno a recuperare e-mail ormai spedite o ricevute siamo di fronte ad un'attività intercettativa»[203].

La tesi si condivide, ma con una precisazione. La captazione furtiva in tanto è legittima, in quanto rientri in un'attività di intercettazione che rispetti le prescrizioni di cui al d.lgs. del 29 dicembre 2017, n. 216. Se, invece, occorre procedere all'acquisizione della corrispondenza elettronica in ossequio alla disciplina dei sequestri, il carattere palese e garantito dell'operazione non sembra potersi conciliare con un'attività occulta e con la tutela costituzionale del segreto epistolare, in assenza di una previsione di legge.

Tuttavia, in tale differenziazione, si rinvengono i sintomi di un'ingiustificata disparità di trattamento.

Alla luce delle considerazioni su esposte, risulta ancor più urgente un intervento normativo o, quantomeno, un consolidamento dell'orientamento giurisprudenziale, che stabilisca criteri oggettivi e certi che consentano di determinare se, nel caso concreto, l'acquisizione della corrispondenza elettronica debba avvenire secondo le regole delle intercettazioni o dei sequestri.

[203] Cass., Sez. IV, 28 giugno 2016, n. 40903, *Grassi ed altri*, cit., p. 39: «*si può concludere che, indipendentemente dal sistema di intrusione utilizzato (quello dell'accesso diretto al computer ovvero occulto attraverso un programma spia), quando si vanno a recuperare e-mail ormai spedite o ricevute siamo di fronte ad un'attività intercettativa*».

6. L'equiparazione giurisprudenziale delle *e-mail* alla prova documentale

Le considerazioni sopra esposte circa la disciplina applicabile in tema di apprensione della corrispondenza elettronica non hanno trovato accoglimento nell'orientamento espresso di recente dalla Sezione quinta della Corte di Cassazione.

I risultati delle indagini, aventi ad oggetto reati fallimentari, si sono basati principalmente sui dati contenuti nel telefono cellulare in uso all'indagata ed estratti a seguito del sequestro probatorio del dispositivo.

La sentenza, depositata il 16 gennaio 2018, merita di essere segnalata per tre profili.

Il primo attiene al riconoscimento dell'ammissibilità del ricorso avverso l'ordinanza del Tribunale del riesame confermativa del sequestro probatorio di uno *smartphone*. L'avvenuta restituzione dello stesso, previa estrazione di una copia del suo contenuto, non fa venir meno l'interesse all'esclusiva disponibilità dei dati. Si riconosce, quindi, l'incidenza prolungata di tale operazione sulla sfera di riservatezza individuale.

Occorre, tuttavia, dimostrare l'esistenza di un interesse concreto ed attuale, oggettivamente apprezzabile, all'utilizzo esclusivo dei dati, in linea con quanto già affermato dalle Sezioni Unite[204]. Nonostante l'esistenza di un onere di allegazione piuttosto stringente a carico dell'interessato, si tratta di un approdo giurisprudenziale degno di apprezzamento, se si considerano le resistenze del passato[205].

In secondo luogo, per quanto concerne la disciplina in materia di apprensione della posta elettronica, la Corte sembra aderire ad un criterio strettamente temporale, nella parte in cui esclude l'applicazione dell'art. 266-*bis,* non essendo riscontrabile un flusso di comunicazioni in tempo reale.

Ad opinione del Collegio, non si tratterebbe nemmeno di "corrispondenza", in mancanza di un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito[206].

---

[204] Cass., Sez. Un., 20 luglio 2017, n. 40963, *Andreucci*, in *C.E.D. Cass.*, n. 270497.
[205] Cass., Sez. VI, 10 giugno 2015 (ud. 24 febbraio 2015), n. 24617, n. 264094.
[206] Cass., Sez. III, 13 gennaio 2016 (udienza 25/11/2015), n. 928, *Giorgi,* cit.

Pertanto, i dati conservati nella memoria di un dispositivo elettronico sottoposto a sequestro vengono appresi e acquisiti al procedimento ai sensi dell'art. 234.[207] La natura di documento, che giustifica l'applicazione della disciplina in tema di prove documentali, riguarda non solo le *e-mail* già spedite e/o ricevute, ma anche i messaggi scambiati mediante l'applicazione *WhatsApp* ed il servizio di messaggistica breve (SMS).

Tuttavia, l'equiparazione *tout court* di dati comunicativi ai documenti tradizionali e l'interpretazione restrittiva della nozione di corrispondenza destano qualche perplessità.

Occorre considerare che l'acquisizione di elementi probatori digitali rappresenta l'esito di un'attività di ricerca della prova. In mancanza di un'operazione di prelevamento di dati, e, quindi, di un sequestro informatico, il contenuto della corrispondenza elettronica resterebbe sconosciuto al processo.

Il mezzo di ricerca della prova rappresenta, dunque, il filtro attraverso cui dati comunicativi rilevanti ai fini dell'accertamento dei fatti entrano nel materiale probatorio. Pertanto, sembrerebbe più opportuno applicare la disciplina in materia di sequestri, non solo in relazione all'apprensione fisica del supporto informatico, ma anche con riferimento al prelevamento e alla duplicazione dei dati ivi contenuti.

In senso difforme alla sentenza qui richiamata, la Sezione quarta nel 2016[208] (vedi *supra*) si è pronunciata a favore di un'applicazione estensiva dell'art. 266-*bis*: l'apprensione delle *e-mail* archiviate nella memoria del dispositivo attenzionato segue le regole in materia di intercettazioni, nonostante la captazione non avvenga in tempo reale. Preso atto dell'esistenza di un contrasto giurisprudenziale all'interno di sezioni diverse della Corte di Cassazione, è ragionevole attendersi una pronuncia del Collegio nella sua composizione più autorevole.

In ultima analisi, il terzo spunto di riflessione offerto dalla sentenza in oggetto riguarda la compatibilità della copia integrale dei dati con il principio di proporzionalità

---

[207] *Contra*, ord. Trib. Modena, 28 settembre 2016. Non può ammettersi una «*svalutazione dei files 'inerenti attività comunicativa in dati decodificati ed allocati nel PC, sfasati cronologicamente con il momento dello scambio comunicativo al fine di considerarli meri documenti presenti nella memoria del PC o del gestore'*». Pertanto, i risultati dell'attività investigativa inerenti alla corrispondenza elettronica vengono considerati inutilizzabili. «*Ci si trova al cospetto di un'area presidiata dall'art. 15 della carta costituzionale con operatività della riserva di legge e di giurisdizione. Le modalità operative attuate dal PM hanno eluso tale riserva violando la segretezza della corrispondenza*».

[208] Cass., Sez. IV, 28 giugno 2016, n. 40903, *Grassi ed altri*, cit.

e adeguatezza dell'atto ablativo[209]. I giudici di legittimità ritengono privo di fondatezza anche questo secondo motivo di gravame, in quanto la copia forense è «*una modalità conforme alla legge, che mira a proteggere, nell'interesse di tutte le parti, l'integrità e l'affidabilità del dato così acquisito*».

La complessità dell'operazione di selezione dei documenti contabili avrebbe richiesto una lunga attività di analisi, non realizzabile *in loco*[210]. L'acquisizione di dati non rilevanti «*non inficia la validità del provvedimento di sequestro, e dunque non può trovare rimedio in questa sede*».

Nonostante il rigetto del ricorso, sembra ammettersi la necessità di garantire un rimedio all'apprensione di dati privi di un legame pertinenziale con il reato.

[209] *Contra*, ord. Trib. Torino, 7 febbraio 2000. Il sequestro di un *computer* viene ritenuto lesivo dei diritti fondamentali del destinatario del provvedimento e dei soggetti in contatto con lui, in quanto risulta «*altamente verosimile che vi siano una serie di e-mail che potrebbero non concernere la fattispecie di reato*».

[210] Cass., Sez. V, 27 ottobre 2016, n. 25527, *Storari,* in *C.E.D. Cass.,* n. 269811.

CAPITOLO V

La novella riguardante le intercettazioni e l'impiego di un "captatore informatico"

Sommario: 1. Brevi cenni a margine della riforma in materia di intercettazioni. - 2. La neo-introdotta disciplina delle intercettazioni tra presenti mediante l'utilizzo di un captatore informatico. - 3. Le intercettazioni tra presenti "semplificate" in relazione ai delitti contro la P.A.

1. Brevi cenni a margine della riforma in materia di intercettazioni

L'esigenza di un intervento del legislatore in materia di utilizzo di strumenti informatici nello svolgimento dell'attività investigativa ha trovato una prima risposta normativa nel decreto legislativo del 29 dicembre 2017, n. 216[211]. Viene così attuata una delle due deleghe contenute nella legge del 23 giugno 2017, n. 103[212], più volte citata.

Più precisamente, l'area dell'intervento governativo viene delimitata dall'art. 1, commi 82, 83 e 84, lettere a), b), c), d) ed e) della legge 103/2017.

L'introduzione nel corso della stesura del presente elaborato, a dimostrazione dell'urgenza della riforma[213], rende possibile un confronto "a caldo" tra le prospettazioni

[211] *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*. G.U. Serie Generale n. 8, 11 gennaio 2018.

[212] *Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario* (GU n. 154 del 4 luglio 2017). Si riporta il testo dell'art. 1, comma 82: «*Il Governo è delegato ad adottare decreti legislativi per la riforma della disciplina in materia di intercettazione di conversazioni o comunicazioni e di giudizi di impugnazione nel processo penale nonché per la riforma dell'ordinamento penitenziario, secondo i principi e criteri direttivi previsti dai commi 84 e 85*».

[213] Prima di tale intervento, diverse proposte di legge avevano posto il tema all'attenzione del legislatore. Nel corso dei lavori parlamentari per la conversione del decreto-legge 18 febbraio 2015, n. 7, recante *Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale*, convertito con modificazioni dalla legge del 17 aprile 2015, n. 43, si era proposto di inserire nell'art. 266 *bis* c.p.p. le parole «*anche attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico*». In seguito, si era proposto di limitare tale strumento alle indagini relative ai delitti di cui agli artt. 270 *bis*, 270 *ter*, 270 *quater* e 270 *quinquies* c.p., commessi con le finalità di terrorismo di cui all'art. 270 *sexies* c.p. Nello stesso verso, la proposta di

sopra esposte e la soluzione normativa. In particolare, si vogliono misurare, senza troppe pretese di precisione, le distanze esistenti tra la disciplina neo-introdotta sull'impiego investigativo di un captatore informatico e le ricostruzioni ermeneutiche che fino ad ora si sono fatte carico della materia.

Ma, la novella non si limita a disciplinare i casi e i modi d'impiego del "nuovo" strumento captativo, in ossequio al principio di tassatività.

Come dimostrano gli artt. 2 e 3 del decreto, il legislatore va oltre il mero adeguamento delle norme all'evoluzione tecnologica (e ad una prassi ormai diffusa).

Si coglie l'occasione per una rivisitazione complessiva delle procedure, nel dichiarato tentativo di assicurare un'adeguata tutela della riservatezza dei soggetti captati e dell'oggetto delle loro comunicazioni o conversazioni.

Il tema è strettamente connesso al rischio che il captatore, seguendo gli spostamenti del dispositivo in uso al soggetto *target*, realizzi una pluralità di intercettazioni tra presenti in luoghi riservati altrui, invadendo la sfera di privatezza di soggetti terzi.

Un tentativo di primo filtraggio dei risultati delle captazioni ad opera degli organi inquirenti ha trovato diverse modalità di attuazione nelle circolari di alcune Procure della Repubblica[214], sintetizzate dal Consiglio superiore della magistratura nella delibera n. 285 del 29 luglio 2016.

Tra le novità più rilevanti occorre segnalare la tendenziale[215] sostituzione dell'udienza di stralcio da un'ordinanza del giudice, emessa in camera di consiglio senza la partecipazione del pubblico ministero e del difensore. Ma, la decisione del giudice

---

legge C. 3470, *Modifiche all'art. 266 bis del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche*.
In data 20 aprile 2016 viene depositata la proposta di legge C. 3762 (*Modifiche al codice di procedura penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, in materia di investigazioni e sequestri relativi a dati e comunicazioni contenuti in sistemi informatici o telematici*), dove si fa riferimento a perquisizioni a distanza e al sequestro da remoto di dati. Da ultimo, la proposta di legge, C. 4260, è stata depositata alla Camera dei Deputati il 31 gennaio 2017. Il 15 marzo 2017, è stato approvato in Senato il disegno di legge n. 2067 (*Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario*), convertito nella legge n. 103, 23 giugno 2017.

[214] Per un'efficace sintesi dei principali modelli che hanno ispirato le circolari cfr. P. TONINI-F. CAVALLI*, Le intercettazioni nelle circolari delle procure della repubblica*, cit., pp.707-708.

[215] Si veda l'art. 268-*quater*, comma secondo: «*Quando è necessario, l'ordinanza è emessa a seguito dell'udienza fissata per il quinto giorno successivo alla scadenza del termine indicato nel comma 1, con tempestivo avviso al pubblico ministero e ai difensori*».

interviene sulla base delle richieste di acquisizione formulate dalle parti, fermo restando il suo ruolo di garante.

Se le parti non si attivano – e l'esperienza delle liste testimoniali rappresenta un caso eloquente di inerzia - il giudice può comunque escludere il materiale manifestamente irrilevante e ordinare lo stralcio dei verbali e delle registrazioni di cui è vietata l'utilizzazione, ai sensi dell'art. 268-*quater*. Il materiale non acquisito viene restituito al pubblico ministero. Gli interessati possono chiederne la distruzione, a tutela della riservatezza.

Infine, viene istituito un apposito archivio riservato presso l'ufficio del pubblico ministero (art. 269 c.p.p.), con accesso limitato al G.i.p. e ai difensori, dove viene custodita tutta la documentazione inerente all'attività captativa, compresi gli atti e i verbali delle comunicazioni e conversazioni non acquisite.

2. La neo-introdotta disciplina delle intercettazioni mediante l'utilizzo di un captatore informatico

L'art. 266, comma secondo, così come riformato dall'art. 4, comma primo, lett. a) del decreto legislativo, consente espressamente l'esecuzione di intercettazioni di comunicazioni tra presenti «*anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile*».

Ne consegue l'accoglimento di quell'indirizzo interpretativo[216] che aveva proposto una lettura ampia della sentenza *Scurato*, nel senso di ammettere le captazioni "elettroniche" di conversazioni o comunicazioni tra presenti anche in relazione ai reati comuni, ferma restando la sussistenza di un fondato motivo per ritenere che l'attività criminosa sia in corso di svolgimento nei luoghi di privata dimora.

Così come previsto dalla delega, il potenziale bersaglio del captatore viene individuato in dispositivi elettronici portatili.

Di qui il primo interrogativo: la specificazione è nel senso di escludere l'installazione del *software* nei dispositivi fissi (elaboratore elettronico, *smart* TV) o si

[216] Cfr. F. CAJANI, *Odissea del captatore informatico*, cit.

può ritenere che questi ultimi siano implicitamente inclusi, in quanto inevitabilmente legati ad un unico domicilio? Sembrerebbe preferibile la seconda soluzione.

Le principali perplessità circa l'impiego di un virus informatico all'interno di un apparecchio mobile erano legate proprio al carattere itinerante dell'operazione captativa che ne sarebbe conseguita. La portabilità del dispositivo infettato comporta, infatti, una potenziale moltiplicazione delle intercettazioni tra presenti all'interno del domicilio di soggetti estranei alle indagini. Il rischio di intercettazioni "peripatetiche" risulta invece assorbito dall'allocazione fissa dell'apparecchio elettronico infettato.

In tal caso, il captatore diviene il moderno sostituto della microspia ed è indissolubilmente legato all'ambiente in cui è installato.

Pertanto, sembra potersi ritenere che l'esclusivo riferimento ai dispositivi portatili non valga ad escludere i dispositivi fissi, aventi una portata invasiva meno ampia e necessariamente circoscritta al luogo di privata dimora indicato nel provvedimento di autorizzazione.

In ogni caso, resta ferma l'estensione al captatore informatico installato in dispositivi fissi delle disposizioni e, soprattutto, delle cautele previste dalla riforma a tutela della riservatezza, nonché dell'affidabilità, sicurezza ed efficacia del programma informatico utilizzato.

Il legislatore delegante non ha tenuto conto della polifunzionalità del captatore informatico. Di qui la regolamentazione esclusiva della funzione di attivazione del microfono, ormai pacificamente ricondotta all'istituto delle intercettazioni.

Del resto, come si è già chiarito *supra* (cfr. Capp. III e IV), non vi è unanimità di vedute circa la possibilità di ricondurre ciascuna delle ulteriori funzionalità del captatore ad una determinata attività di ricerca della prova.

Si osservi che il riferimento a tale funzione compare solo nell'art. 267, comma primo: nel decreto di autorizzazione occorre determinare i luoghi ed il tempo, in relazione ai quali è consentita l'attivazione del microfono.

Per quanto concerne le restanti disposizioni introdotte, sembra darsi per scontato che l'esecuzione di un'intercettazione tra presenti mediante l'impiego di un programma informatico possa avvenire a seguito di attivazione dell'amplificatore acustico.

Ai sensi del nuovo comma 2-*bis* dell'art. 266, l'intercettazione *inter praesentes* nei luoghi indicati dall'art. 614 c.p. (anche mediante l'inserimento di un captatore

informatico) è «*sempre consentita nei procedimenti per i delitti di cui all'art. 51, commi 3-bis e 3-quater*». Come si vede, gli stessi reati che valgono a radicare la competenza in capo alla Procura distrettuale giustificano il ricorso agevolato all'agente intrusore.

Dunque, si restringe, rispetto alle Sezioni Unite *Scurato*, la nozione di criminalità organizzata rilevante ai fini dell'applicazione della disciplina derogatoria di cui all'art. 13 del decreto-legge del 13 maggio 1991, n. 152, convertito nella legge del 12 luglio 1991, n. 203.

Il legislatore ha quindi accolto le critiche riguardanti l'eccessiva ampiezza di una nozione giurisprudenziale estesa ai «*reati comunque facenti capo ad un'associazione per delinquere, ex art. 416 cod. pen., correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato*».

Ma la portata garantistica del ridimensionamento entro confini certi della nozione di criminalità organizzata subisce una battuta d'arresto con l'estensione della disciplina derogatoria ad essa relativa nei procedimenti per i più gravi reati dei pubblici ufficiali contro la pubblica amministrazione.

Quanto ai requisiti del decreto di autorizzazione, l'art. 4 del decreto legislativo 216/2017 modifica l'art. 267, in relazione ai presupposti e alle forme del provvedimento.

Si conferma l'orientamento espresso dalle Sezioni Unite *Scurato,* che prende le distanze dalla sentenza *Musumeci*, nella parte in cui esclude la necessaria indicazione del luogo all'interno del decreto che dispone l'intercettazione tra presenti mediante l'utilizzo del captatore, in relazione ai reati di criminalità organizzata.

Occorre, tuttavia, indicare «*le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini*».

Se, invece, il procedimento ha ad oggetto reati diversi da quelli di cui all'art. 51, commi 3-*bis* e 3-*quater*, il provvedimento autorizzativo deve contenere la determinazione, anche indiretta, dei luoghi e del tempo in relazione ai quali è consentita l'attivazione del microfono.

Il riferimento al tempo implica un funzionamento del programma informatico ad intervalli predeterminati, come già proposto da una parte della dottrina[217].

Nello stesso senso, la previsione dell'attivazione della funzione previo comando da remoto.

[217] Si veda *supra* cap. II, § 2.

Non basta la mera installazione all'interno del dispositivo: il programma deve essere attivato e, infine, disattivato «*con modalità tali da renderlo inidoneo a successivi impieghi*»[218], dandone atto nel verbale. A tal fine, la polizia giudiziaria può avvalersi di persone idonee, ai sensi dell'art. 348, comma quarto.

In funzione garantistica e preventiva di eventuali dibattiti sul punto, il nuovo comma 1-*bis* dell'art. 271 prevede la sanzione dell'inutilizzabilità in relazione ai dati acquisiti nel corso delle operazioni preliminari di inserimento del captatore ovvero in caso di superamento dei limiti di tempo e di luogo stabiliti nel decreto autorizzativo.

Infine, il programma impiegato e i luoghi in cui in concreto si svolgono le comunicazioni o conversazioni saranno indicati nel verbale di cui all'art. 89, comma primo, come modificato dall'art. 5, comma primo, lett. a), n. 1)[219].

A tutela della riservatezza, l'art. 268, comma 2-*bis*, prevede oggi il divieto di trascrizione, anche sommaria, «*delle comunicazioni o conversazioni irrilevanti ai fini delle indagini, sia per l'oggetto che per i soggetti coinvolti, nonché di quelle, parimenti non rilevanti, che riguardano dati personali definiti sensibili dalla legge*». La trascrizione viene sostituita dall'indicazione della data, dell'ora e del dispositivo su cui la registrazione è avvenuta[220].

Inoltre, il materiale rilevante viene preventivamente selezionato dal pubblico ministero, controllato dal difensore e, infine, sottoposto al vaglio del giudice, che procede all'acquisizione delle conversazioni o comunicazioni indicate delle parti.

Tale schema mira, da un lato ad uno snellimento della procedura, dall'altro a prevenire *ex ante* l'ingresso di materiale irrilevante o strettamente personale. Il che è altamente probabile che si verifichi quando venga impiegato il captatore informatico.

Tuttavia, occorre osservare che tale procedura partecipata viene meno nel caso in cui venga introdotta la fase cautelare. L'acquisizione del materiale posto a sostegno della richiesta di applicazione di una misura cautelare viene disposta unilateralmente da parte

---

[218] Art. 89, comma 2-*quinquies*, disp. att. c.p.p., come modificato dal d.lgs. 216/2017, art. 5, *Modifiche alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale*.

[219] «*Quando si procede ad intercettazione delle comunicazioni e conversazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile, il verbale indica il tipo di programma impiegato e i luoghi in cui si svolgono le comunicazioni o conversazioni*».

[220] I verbali delle operazioni vengono trasmessi al pubblico ministero per la conservazione nell'archivio riservato di cui all'art. 269, comma primo.

del pubblico ministero[221], con inserimento dei verbali nel fascicolo di cui all'art. 373, comma quinto. Cessa, a questo punto, il segreto sugli atti.

La rinuncia ad un'adeguata tutela della riservatezza in materia cautelare incide considerevolmente sulla dichiarata portata garantistica della riforma[222], segnandone un significativo restringimento. A tal proposito, si tenga conto che i risultati derivanti dall'impiego investigativo del captatore hanno un peso specifico considerevole in relazione al procedimento *de libertate*, come si può dedurre dai casi concreti sopra esaminati.

3. Le intercettazioni di comunicazioni tra presenti "semplificate" in relazione ai delitti contro la P.A.

Tra i principi direttivi della legge 103/2017, compare la previsione della «*semplificazione delle condizioni per l'impiego delle intercettazioni delle conversazioni e delle comunicazioni telefoniche e telematiche nei procedimenti per i più gravi reati dei pubblici ufficiali contro la pubblica amministrazione*»[223].

L'utilizzo di un captatore informatico può rivelarsi particolarmente utile in tale contesto, soprattutto se si ricorre all'accensione della video camera, poiché consente di cristallizzare condotte illecite di difficile tracciabilità, come lo scambio di una tangente.

L'art. 6 del d.lgs. 216/2017 prevede l'applicazione dell'art. 13 d.l. 152/1991 ai procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione «*puniti*

---

[221] La legge 103/2017, art. 1, comma 84 lett. a), n. 1, prescrive che «*ai fini della selezione del materiale da inviare al giudice a sostegno della richiesta di misura cautelare, il pubblico ministero, oltre che per necessità di prosecuzione delle indagini, assicuri la riservatezza anche degli atti contenenti registrazioni di conversazioni o comunicazioni informatiche o telematiche inutilizzabili a qualunque titolo ovvero contenenti dati sensibili ai sensi dell'articolo 4, comma 1, lettera d), del codice di cui al decreto legislativo 30 giugno 2003, n. 196, che non siano pertinenti all'accertamento delle responsabilità per i reati per cui si procede o per altri reati emersi nello stesso procedimento o nel corso delle indagini, ovvero irrilevanti ai fini delle indagini in quanto riguardanti esclusivamente fatti o circostanze ad esse estranei*».

[222] G. SPANGHER, *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, in *Giur. pen. Web*, 2018, n. 1. «*Invero, non esiste un controllo preliminare sulle intercettazioni che il pubblico ministero manda al giudice a sostegno della richiesta delle misure coercitive. Tra queste potrebbero essere ricomprese non solo quelle che il giudice potrebbe ritenere, seppur attinenti ai fatti di cui alle indagini, non significativi ai fini delle misure richieste, ma anche i brogliacci contenenti elementi del tutto estranei*».

[223] Legge 103/2017, art. 1, comma 84, lett. d).

con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 del codice di procedura penale».

La soluzione proposta dal legislatore delegato non pare realizzare il miglior bilanciamento degli interessi in gioco. L'ampliamento dei poteri d'indagine attraverso il rinvio ad una disposizione eccezionale non assicura piena aderenza al principio di proporzionalità e di legalità.

Inoltre, la pena non inferiore nel massimo a cinque anni è comminata per la maggioranza dei delitti di cui al Capo I del Titolo II del codice penale[224], di recente riformato dalla legge del 27 maggio 2015, n. 69, che ha previsto un innalzamento del minimo e del massimo della pena di molti reati[225].

Non possono ammettersi estensioni così agevolate di una disciplina eccezionale e derogatoria, quale quella di cui al d.l. 152/1991, per rispondere ad esigenze contingenti, per quanto non si neghi l'esistenza di un contesto di criminalità organizzata spesso sotteso ai reati contro la pubblica amministrazione.

L'unico limite è costituito dall'impossibilità di effettuare una captazione occulta nei luoghi di privata dimora mediante un programma informatico installato in un dispositivo portatile, «*quando non vi è motivo di ritenere che ivi si stia svolgendo l'attività criminosa*» (art. 6, comma secondo).

Si noti la formulazione in negativo e l'elisione dell'aggettivo fondato, che indeboliscono significativamente la tutela del domicilio.

Peraltro, resta comunque ferma la possibilità di eseguire un'intercettazione, per così dire, tradizionale, in presenza di sufficienti indizi.

L'applicazione della disciplina derogatoria risulta, quindi, parziale, dal momento che, in relazione alle captazioni occulte nei luoghi di cui all'art. 614 c.p., viene apprestata una tutela più significativa rispetto alla disciplina di cui al d.l. 152/ 1991.

Tuttavia, la norma, a differenza dell'art. 266, comma secondo, non subordina l'ammissibilità delle intercettazioni tra presenti nei luoghi di privata dimora al «*fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa*».

---

[224] Resterebbero esclusi dalla semplificazione delle condizioni per il ricorso alle intercettazioni di conversazioni e di comunicazioni telefoniche e telematiche gli artt. 316, 316-*bis*, 316-*ter*, 319-*quater*, comma 2, 322, 323, 326, 328 del codice penale.

[225] Per approfondimenti sulla portata de "*La nuova riforma in tema di delitti contro la P.A., associazioni di tipo mafioso e falso in bilancio*" si veda F. CINGARI, *Una prima lettura delle nuove norme penali a contrasto dei fenomeni corruttivi*, in *Diritto penale e processo*, 2015, n. 7, pp. 803 ss.

Dal dato normativo, pare bastevole un mero sospetto circa l'attuale svolgimento dell'attività illecita ai fini dell'impiego del captatore informatico. La tutela apprestata si colloca, quindi, su di un livello inferiore rispetto alle regole ordinarie di cui all'art. 266, comma secondo[226].

Infine, si osservi che a differenza di quanto previsto in relazione agli artt. 2,3,4, 5 e 7, l'entrata in vigore dell'art. 6 non è rinviata ai provvedimenti autorizzativi emessi dopo il centottantesimo giorno successivo alla data di entrata in vigore del decreto (art. 9). Conseguentemente, segue le regole ordinarie.

[226] L'art. 4, comma primo, lett. a), n. 1), modifica l'art. 266, comma secondo, primo periodo, aggiungendo: «*che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile*».

CONCLUSIONI

Nelle pagine che precedono si è visto come la declinazione dinamica delle indagini elettroniche, resa possibile dall'utilizzo di un captatore informatico, interessi, a vari livelli, le intercettazioni, le ispezioni, le perquisizioni ed i sequestri.

Con riguardo all'ammissibilità della captazione occulta digitale di conversazioni o comunicazioni tra presenti, sono state esposte le linee guida tracciate dalle Sezioni Unite nella sentenza "*Scurato"*, che ha ricondotto alla categoria delle intercettazioni tra presenti, eventualmente domiciliari, quelle realizzate mediante un *virus* informatico installato su di un cellulare e ne ha ammesso, entro certi limiti, la praticabilità. Sono state altresì esaminate le opinioni espresse al riguardo dalla dottrina, parte della quale ha proposto di bilanciare l'ammissione di intercettazioni a mezzo *virus* con l'accorgimento tecnico consistente nell'assicurare una attivazione non permanente della funzione di accensione del microfono. Al riguardo, poi, si è visto come un ruolo fondamentale in chiave garantistica sia ricoperto dal decreto di autorizzazione emesso dal giudice delle indagini preliminari, di cui si è tentato di ricostruire i requisiti essenziali, quando si realizzano intercettazioni mediante captatore informatico. La conferma della potenziale conformità alla legge dell'utilizzo di un captatore informatico, accompagnata da un'estensione delle ipotesi in cui è ammesso, è peraltro giunta nel corso della stesura con il decreto legislativo del 29 dicembre 2017, n. 216, pubblicato in Gazzetta Ufficiale in data 11 gennaio 2018, che ha riformato le disciplina relativa alle intercettazioni.

Invece, in relazione agli altri mezzi di ricerca della prova (ispezioni, perquisizioni e sequestri), si è assunto come punto di partenza dell'analisi, volta a considerare ammissibili o meno forme di ricerca probatoria *online*, la legge del 18 marzo 2008, n. 48, attuativa della Convenzione di Budapest sulla criminalità informatica, che ha novellato talune disposizioni codicistiche in materia, estendendo l'oggetto di ispezioni, perquisizioni e sequestri anche ai dati digitali e prevedendo talune specifiche norme sul punto.

Dall'esame di tali norme, non ci è parso potersi ammettere un'estensione delle fattispecie ivi previste anche ad ispezioni, perquisizioni e sequestri realizzati mediante captatore informatico, benché la prassi investigativa evidenzia molteplici casi di ricorso a tali operazioni.

La novella apportata con la citata legge n. 48 del 2008 appare limitata ad un'operazione statica sul dato digitale, archiviato nella memoria del sistema informatico o telematico attenzionato. Ma l'ostacolo principale per l'interprete è costituito dal carattere occulto della sorveglianza *online* che il captatore intende realizzare, a cui occorre aggiungere la capacità di agire da "copiatore informatico", mediante l'attivazione della funzione di acquisizione in copia dei dati contenuti nel dispositivo bersagliato, con la realizzazione di un vero e proprio sequestro digitale.

L'attività ispettiva, perquisitiva ed apprensiva, per quanto a "sorpresa", è palese e garantita, come si può ricavare dalla normativa vigente e dalla tradizione giuridica.

Di conseguenza, non sembra potersi ammettere, per via interpretativa, una denaturazione di tali istituti giuridici, incompatibile con un'adeguata tutela dei diritti coinvolti e sproporzionata rispetto allo scopo perseguito.

Pertanto, *de iure condendo*, il ricorso a tale programma informatico, se assolutamente indispensabile per lo svolgimento delle indagini, deve necessariamente essere adeguato all'istituto giuridico in cui è calato. Ne consegue che l'interessato deve essere informato, nel più breve tempo possibile, dell'operazione che s'intende compiere, lesiva del diritto alla riservatezza informatica. In altre parole, sembrerebbe opportuno rendere palese l'attività investigativa digitale, al fine di consentire l'esercizio del diritto di difesa e l'attivazione del contraddittorio.

Medio tempore, in assenza di un'espressa previsione di legge e di un provvedimento motivato che attui un adeguato contemperamento degli interessi in gioco, si formerebbe una prova, prima ancora che inutilizzabile, incostituzionale.

Quel processo di accelerazione della ricerca del dato digitale, innescato dal captatore informatico, in funzione di catalizzatore dei mezzi di ricerca della prova, può essere efficacemente inibito soltanto dall'azione dei diritti costituzionali, garanti della legalità e dell'attendibilità del risultato.

Le innovazioni, se non misurate sui diritti, rischiano di trasformare il progresso in regresso. In questa direzione, le indagini informatiche non possono tradursi in indagini occulte, in evidente contrasto con i principi generali dell'ordinamento.

Se gli istituti giuridici, così come riformati o come non riformati dal legislatore, siano in grado di sopravvivere alle nuove sfide contemporanee, solo il tempo potrà rivelarlo. Pare conservare ancora attualità quella concezione gattopardiana secondo cui «*se vogliamo che tutto rimanga com'è, bisogna che tutto cambi*».

Di fronte all'impossibilità di arrestare l'invasione nel procedimento penale dell'evoluzione tecnologica, il vano tentativo di preservare le tradizionali modalità di attuazione dei mezzi di ricerca della prova rischia, paradossalmente, di causare un'erosione delle fondamenta del diritto processuale penale. Lo stesso legislatore, non a caso, non ha predeterminato i modi d'impiego degli strumenti investigativi tipici, così da rendere possibile un progressivo adeguamento alla modernità.

Di fronte ad una prassi insistente nel ricorrere al captatore informatico, sostenere l'inammissibilità *tout court* dello strumento non conduce ad alcun esito soddisfacente.

Gli sforzi interpretativi dovrebbero piuttosto convergere verso l'individuazione di eventuali limitazioni da imporre alle condizioni e alle modalità di impiego, in modo da prevedere garanzie ulteriori rispetto a quelle già esistenti.

Quando si potrà ritenere raggiunto, con ragionevole certezza, il miglior bilanciamento tra l'esigenza di accertamento dei reati e la protezione dei diritti individuali, allora potrà dirsi instaurato un legame solido e condiviso tra tecnologia e processo.

BIBLIOGRAFIA

AMATO G., *Reati di criminalità organizzata: possibile intercettare conversazioni o comunicazioni con un "captatore informatico"*, in *Guida dir*., 2016, n. 34-35, p. 79.

APRILE E. - SPIEZIA F., *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche*, Milano, 2004, p. 104.

APRILE E., *Intercettazioni di comunicazioni*, in A. SCALFATI (a cura di), *Prove e misure cautelari*, in *Trattato di procedura penale*, diretto da G. SPANGHER, vol. II, tomo I, Torino, 2009, p. 535.

ATERNO S., *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, n. 4, pp. 966-967.

BALDUCCI P., *Perquisizioni*, in *Enc. dir.*, IV, Milano, 2000, p. 982.

BALSAMO A., *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte Europea*, in *Cass. pen*., 2016, n. 5, pp. 2274 ss.

BARILE P. – CHELI E., *Corrispondenza [libertà di]*, *Enc. dir*., X, Milano, 1962, pp. 744, 745.

BARROCU G., *Il captatore informatico: un virus per tutte le stagioni, in Dir. pen. proc.*, 2017, n. 3, pp. 379 ss.

BASSO E., *Art. 249*, in *Commento al nuovo codice di procedura penale*, coordinato da M. CHIAVARIO, II, Torino, 1990, p. 715.

BATTINIERI L., *La perquisizione online tra esigenze investigative e ricerca atipica della prova*, in *Sicurezza e Giustizia*, 2013, n. 4, p. 45.

BERNARDI S., *Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art. 624 bis c.p.*, in *Diritto penale contemporaneo* (*web*), 4 luglio 2017 (ultimo accesso: 7 ottobre 2017).

BONO G., *Il divieto di indagini ad explorandum include i mezzi informatici di ricerca della prova*, in *Cass. pen.*, 2013, n. 4, pp. 1530-1531.

BRAGHÒ G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della convenzione di Budapest sul cybercrime*, Milano, 2009, p. 194.

CAPRIOLI F., *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista Brasileira de Direito Processual Penal*, 2017, vol. 3, n. 2, pp. 483-510.

CAJANI F., *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, gennaio 2010, consultabile online: http://www.marcomattiucci.it/informatica_digitalforensics_l482008.php

CAJANI F., *Odissea del captatore informatico*, in *Cass. pen*., 2016, p. 4143.

CAMON A., *Cavalli di Troia in Cassazione*, *Arch. nuova proc. pen*., 2017, n. 1, p. 93.

CAMON A., *Le intercettazioni nel processo penale*, Milano, 1996, p. 12, p. 67.

CAMON A., *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove incostituzionali*, in *Cass. pen.* 1999, p. 1192 ss.

CANZIO G., *Prova scientifica, ricerca della «verità» e decisione giudiziaria nel processo penale, in Decisione giudiziaria e verità scientifica*, Milano, 2005, p. 60, 64.

CARLI L., *Le indagini preliminari nel sistema processuale penale*, II ed., Milano, 2005, p. 333.

CAVINI S., *Il riconoscimento informale di persone o di cose come mezzo di prova atipico*, *Dir. pen. proc*., 1997, p. 838.

CERQUA F., *Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica*, in *Dir. pen. cont.* [*web*], 23 luglio 2015 (ultimo accesso: 28 gennaio 2018).

CINGARI F., *Una prima lettura delle nuove norme penali a contrasto dei fenomeni corruttivi*, in *Diritto penale e processo*, 2015, n. 7, pp. 803 ss.

CISTERNA A., *Spazio ed intercettazioni, una liason tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni Unite*, in *Arch. pen*., 2016, n. 2, p. 331 ss.

CONSO G., *La criminalità organizzata nel linguaggio del legislatore*, in *Giust. pen*., III, 1992, p. 392.

CONSO G. – GREVI V.- BARGIS M., *Compendio di procedura penale*, VIII ed., Padova 2016, pp. 286, 525.

CONTI C., *Iudex peritus peritorum e il ruolo degli esperti nel processo penale*, in *Dir. pen. proc*., 2008, p. 31.

CORONA F., *Perquisizioni di sistema informatico per le prenotazioni dei voli online: i dati devono essere già presenti*, in *Sicurezza e Giustizia*, 2015, n. 3.

CUOMO L.-RAZZANTE R., *La nuova disciplina dei reati informatici*, Torino, 2009, p. 59.

CURTOTTI NAPPI D., *I collegamenti audiovisivi nel processo penale*, Milano, 2006, p. 117.

DALIA A., *Sequestro penale*, in VASSALLI G. (a cura di), *Dizionario di diritto e procedura penale*, Milano, 1986, p. 939.

DANIELE M., *La prova digitale nel processo penale*, in *Riv. dir. proc*., 2011, n. 2, pp. 283.

DE FLAMMINEIS S., *Le intercettazioni telematiche*, in *Dir. pen. proc*., 2013, p. 992.

DI BITONTO M. L., *Le riprese video domiciliari al vaglio delle Sezioni Unite*, in *Cass. pen*., 2006, p. 3950 ss.

DI BITONTO M. L., *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. Internet*., 2008, p. 503 ss.

DI PAOLO G., *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare ed altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, in *Cass. pen.*, n. 3, 2008, p. 1227.

DOMINIONI O., *In tema di nuova prova scientifica*, in *Dir. pen. proc*., 2001, p. 1062.

FELICIONI P., *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Processo penale e giustizia*, 5, 2016, p. 124.

FELICIONI P., *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Processo penale e giustizia*, 2016, n. 5, pp. 123, 124, 132.

FELICIONI P., *Le ispezioni e le perquisizioni*, in *Trattato di procedura penale*, diretto da G. UBERTIS - G. M. VOENA, Milano, 2012, pp. 89, 282.

FILIPPI L., *L'intercettazione di comunicazioni*, Milano, 1997, p. 82.

FILIPPI L., *sub art. 266-bis*, in A. GIARDA – G. SPANGHER (a cura di), *Codice di procedura penale commentato*, I, Milano, 2010, p. 2635.

FILIPPI L., *L'ispe-perqui-intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi ma sbagliano la terapia (a proposito del captatore informatico)*, *Arch. pen*., 2016, n. 2, pp. 348 ss.

FLOR R., *Brevi riflessioni a margine della sentenza del 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 sostanziale*, in *Riv. trim. dir. pen. ec*., 2009, p. 697 ss.

FLOR R., *Phishing, identity theft, e identity abuse*: *le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen*., 2007.

GENTILE D., *Tracking satellitare mediante gps: attività atipica di indagine o intercettazione di dati?*, *Diritto Penale e Processo*, 12, 2010, p. 1468.

GIORDANO L., *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Diritto penale contemporaneo*, 2017, n. 3.

GIORDANO L., *L'uso di captatori informatici nelle indagini di criminalità organizzata*, in *Cass. pen*., 2017, suppl. n. 5, p. 214.

GIORDANO L., *La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità*, in *Diritto penale contemporaneo*, 2017, n. 9.

GIUNTA F., *Questioni scientifiche e prova scientifica tra categorie sostanziali e regole di giudizio*, in *Criminalia*, 2014, pp. 561 e ss.

IOVENE F., *Perquisizioni e sequestro di computer: un'analisi comparatistica*, in *Riv. dir. proc*., 2012, n. 6, pp. 1067 ss.

JONES M., *The Civilian Batterfield, Protecting GNSS Receivers from Interference and Jamming*, in *InsideGNSS*, march/april, p. 40 ss., consultabile online: http://www.insidegnss.com/auto/marapr11-Jones.pdf.

KERR O. S., *Searches and Seizures in a Digital World*, in 199 *Harvard Law Review* 531 (2005), 558.

LASAGNI G., *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti*", *Commento a Cass. pen., Sez. Un., sent. 28 aprile 2016 (dep. 1 luglio 2016), n. 26889, Pres. Canzio, Rel. Romis, Imp. Scurato*, § 3.4, in *Dir. pen. cont*. (*web)*, 7 ottobre 2016. Ultimo accesso: 29 dicembre 2017.

LEONE G., *Trattato di diritto processuale penale*, II, Napoli, 1961, p. 189.

LOGLI A., *Sequestro probatorio di un personal computer*. *Misure ad explorandum e tutela della corrispondenza elettronica*, in *Cass. pen*., 2008, n. 7/8, p. 2955, nota 6.

LORENZETTO E., *Le attività urgenti di investigazione informatica e telematica*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, p. 154.

LORENZETTO E., *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen*., 2010, n. 4, pp. 1522 ss.

LUPARIA L., *Disciplina processuale e garanzie difensive*, in L. LUPARIA – G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, pp. 108, 135, 136, 162, 163, 164, 172, 173.

LUPARIA L., *La ratifica della Convenzione cybercrime del Consiglio d'Europa. Legge del 18 marzo del 2008, n. 48. I profili processuali*, in *Dir. pen. proc*., 2008, p. 720.

MACCHIA A., *I diritti fondamentali "minacciati": lo sfondo delle garanzie in costituzione*, 2017, in *Diritto Penale Contemporaneo*.

MACRILLÒ A., *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. Int*., 2008, pp. 513, 514.

MANCUSO E. M., *L'acquisizione dei contenuti e-mail*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, pp. 56, 69, 73, 81, 82.

MARIOTTI S. –TACCONI S., *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni VoIP*, in *Diritto dell'Internet*, 2008, n. 6, pp. 558- 562.

MOLINARI F.M., *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2012, n. 2, pp. 703, 709, 711.

MOLINARI F.M., *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, n. 3, pp. 1259 ss.

MOSCARINI P., *Ispezione giudiziale (dir. proc. pen.)*, in *Enc. dir*., agg. II, 1998.

MOSCARINI P., *Lineamenti al sistema istruttorio penale*, Torino, 2017, pp. 23, 46, 88, 107, 108.

NAZZARO G., *La localizzazione del target per l'Autorità Giudiziaria*, in *Sicurezza e Giustizia*, n. 2, 2012, consultabile online: www.ellis.org.

ORLANDI R., *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *Riv. It. dir. e proc. pen*., 2014, p. 1134 ss.

ORLANDI R., *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc*., 2009, p. 135.

PARODI C., *VoIP, Skype e tecnologie d'intercettazione: quali riposte d'indagine per le nuove frontiere di comunicazione?*, in *Diritto penale e processo*, 2008, n. 10, pp. 1309, 1313.

PASCUCCI N., *La ricognizione fotografica*, in *Rivista Italiana Diritto e Procedura penale*, 1, 2017, p. 290.

PECORELLA C., *Diritto penale dell'informatica*, Padova, 2006, p. 294.

PERETOLI P., *Controllo satellitare con GPS: pedinamento o intercettazione?*, in *Dir. pen. proc.*, 2003, p. 95.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Cedam, Padova, 2004, p. 180.

PIO E., *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, in *Parola alla difesa*, 2016, n.1, p. 164 ss.

PITTIRUTI M., *Profili processuali della prova informatica*, in L. MARAFIOTI – G. PAOLOZZI (a cura di), *'Incontri ravvicinati' con la prova penale. Un anno di seminari a Roma Tre*, Torino, 2014, pp. 55-56.

RUGGIERI F., *Profili processuali nelle investigazioni informatiche*, in L. PICOTTI (a cura di), *Il diritto penale nell'epoca di Internet*, Padova, 2004, pp. 160-161.

SCHENA G., *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, in *Cass. pen.* 2016, n. 1, pp. 302, 306.

SERRANI A., *Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie*, in *Arch. Pen.*, 3, 2013, p. 10

SIRACUSANO F., *La prova informatica, in Investigazioni e prove transnazionali*, XXX Convegno Nazionale, Associazione tra gli studiosi del processo penale "G. D. Pisapia", Roma 20-21 ottobre 2016, Università La Sapienza, p. 4.

SPANGHER G., *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, in *Giur. pen. Web*, 2018, n. 1.

TONINI P., *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 406.

TONINI P., *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Dir. pen. e proc*., 2011, p. 1341 in P. MOSCARINI, *Lineamenti del sistema istruttorio penale*, Torino, 2017, p. 103, nota 46.

TONINI P., *Manuale di procedura penale*, p. 237 in P. MOSCARINI, *Lineamenti del sistema istruttorio penale,* Torino, 2017, p. 18, nota 41.

TONINI P., *Progresso tecnologico, prova scientifica e contraddittorio*, in DE CATALDO NEUBURGER L. (a cura di), *La prova scientifica nel processo penale,* Padova, 2007, pp. 65, 57.

TONINI P.-CAVALLI F., *Le intercettazioni nelle circolari delle procure della repubblica*, in *Diritto penale e processo*, 2017, n. 6, pp. 705 ss.

TORRE M., *Il virus di stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali: mezzi di ricerca della prova*, in *Dir. pen. proc*., 2015, n. 9, p. 1167.

TROGU M., *Le intercettazioni di comunicazioni a mezzo Skype,* in *Processo penale e Giustizia,* n. 3, 2014, pp. 104, 108.

TROGU M., *Sorveglianza e "perquisizione" online su materiale informatico*, in SCALFATI A. (a cura di), *Le indagini atipiche,* Torino, 2014, pp. 442 e 445.

UBERTIS G., *La prova scientifica e la nottola di Minerva*, in L. DE CATALDO NEUBURGER (a cura di), *La prova scientifica nel processo penale,* 2007, p. 87.

UBERTIS G., *Prova scientifica e processo penale*, in *Riv. dir. proc. pen.*, a. LIX, n. 3, 2016, p. 1200.

VACIAGO G., *Digital evidence. I mezzi di ricerca della prova digitale e le garanzie dell'indagato*, Torino, 2012, p. 81

VENEGONI A. – GIORDANO L., *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*. (*web*), 8 maggio 2016 (ultimo accesso: 17 gennaio 2018).

ZACCHÈ F. *La prova documentale*, UBERTIS G. – VOENA G.P. (diretto da), *Trattato di procedura penale*, Milano, XIX, 2012, p. 35.

ZACCHÈ F., *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 2013, n. 4, pp. 106, 109.

ZICCARDI G., *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA, *Sistema penale e criminalità informatica*, Milano, 2009, p. 167.

ZONARO M., *Il Trojan - Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento di intercettazione*, in *Parole alla difesa*, 2016, n. 1, p. 164.

RIFERIMENTI GIURISPRUDENZIALI

Corte Cost., sent. n. 85, 9 aprile 2013, in *Giur. Cost.*, 2013, p. 1424 ss.

Corte Cost., 15 gennaio 2013 (ud. 4 dicembre 2012), n. 1.

Corte Cost., 30 novembre 2009, n. 317.

Corte Cost., 24 aprile 2002, n. 135, in *Giur. Cost*., 2002, p. 1062 ss.

Corte Cost. 17 luglio 1998, n. 281, § 3.

Corte Cost., 11 marzo 1993, n. 81.

Corte Cost., 4 aprile 1973, n. 34.

Cass. pen., Sez. Un., 7 settembre 2017, (udienza 20 luglio 2017), n. 40963, *Andreucci*, in *C.E.D. Cass*., n. 270497.

Cass. pen., Sez. Un., 22 giugno 2017 (ud. 23 marzo 2017), n. 31345, in *Foro it.*, 2017, II, 673.

Cass. pen., Sez. Un., c.c. 28 aprile 2016, n. 26889, *Scurato*, in *C.E.D. Cass.*, n. 266906.

Cass. pen., Sez. Un., 15 luglio 2010, n. 37501, *Donadio*, in *C.E.D. Cass.*, n. 247994.

Cass. pen., Sez. Un., 23 aprile 2009, n. 23868, *Fruci*, in *C.E.D. Cass.*, n. 243416.

Cass. pen., Sez., Un., 26 giugno 2008, n. 36359, in *Cass. pen.*, 2009, p. 30.

Cass. pen., Sez. Un., 18 dicembre 2006, *Greco*, n. 41281, in *Guida al Dir.*, 2007, n. 2, p. 86.

Cass. pen., Sez. Un., 28 marzo 2006, n. 26795, *Prisco*, in *C.E.D. Cass*., n. 234270.

Cass. pen., Sez. Un., 22 marzo 2005, n. 17706, in *C.E.D. Cass.*, n. 230895.

Cass. pen., Sez. Un., 28 gennaio 2004, *Ferazzi*, in *Cass. pen*., 2004, p. 1913 ss.

Cass. pen., Sez. Un., 28 maggio 2003, *Torcasio*, in *Cass. pen*., 2004, p. 2094.

Cass. pen., Sez., Un., 23 febbraio 2000, n. 6, in *Cass. pen.*, 2000, p. 2959.

Cass. pen., Sez. Un., 13 luglio 1998, n. 21, *Gallieri*, in *C.E.D. Cass.*, n. 211117.

Cass. pen., Sez. V, 16 gennaio 2018 (udienza 21 novembre 2017), n. 1822.

Cass. pen., Sez. II, 10 novembre 2017 (ud. 18 ottobre 2017), n. 51446, inedita.

Cass. pen., Sez. V, 20 ottobre 2017, n. 48370 (udienza 30 maggio 2017), *Occhionero*.

Cass. pen., Sez. VI, 13 giugno 2017, n. 36874, *Romeo*, inedita.

Cass. pen., Sez. V, 27 ottobre 2016, n. 25527, *Storari*, in *C.E.D. Cass.*, n. 269811.

Cass. pen., Sez. VI, 1 marzo 2016, n. 21740, *Masciotta*, in *C.E.D. Cass.*, n. 26692.

Cass. pen., Sez. IV, 28 giugno 2016, n. 40903, *Grassi ed altri*, in *C.E.D. Cass*., n. 268228.

Cass. pen., Sez. VI, 10 giugno 2015 (ud. 24 febbraio 2015), n. 24617, in *C.E.D. Cass*., n. 264094.

Cass. pen., Sez. III, 9 marzo 2016, n. 17193, *Calabrò*, non mass.

Cass., Sez. V, 4 marzo 2016, n. 26817, in *C.E.D. Cass*., n. 267889.

Cass. pen., Sez. III, 15 gennaio 2016, n. 31415, in *Cass. pen*., 2016.

Cass. pen., Sez. III, 13 gennaio 2016 (udienza 25 novembre 2015), n. 928, *Giorgi*, in *C.E.D. Cass.*, n. 265991.

Cass. pen., Sez. III, 10 novembre 2015, n. 50452, *Guarnera ed altri*, in *C.E.D. Cass*., n. 265615.

Cass., Sez. III, 18 giugno 2015, n. 36927, in *C.E.D. Cass*., 2016, n. 265023.

Cass. pen., Sez. VI, 26 maggio 2015, n. 27100, *Musumeci*, in *C.E.D. Cass.*, n. 265654.

Cass. pen., Sez. V, 29 ottobre 2014, n. 52075.

Cass. pen., Sez. VI, 2 aprile 2014, n. 33229, *Visca*, in *C.E.D Cass*., n. 260339.

Cass. pen., Sez. V, 21 febbraio 2014, n. 16397, in *C.E.D. Cass*., n. 259552.

Cass., Sez. VI, 8 maggio 2013 (ud. 16 aprile 2013), n. 19783, in *Foro It.*, 2014, II, 2, 90.

Cass., Sez. II, 11 aprile 2013, n. 24925, in *C.E.D. Cass*., n. 256540.

Cass. pen., Sez. V, 26 ottobre 2012, n. 42021, in *Foro It*., 2012, II, 709.

Cass. pen., Sez. VI, 25 settembre 2012, n. 41514, *Adamo*, in *C.E.D. Cass.*, n. 253805.

Cass. pen., Sez. IV, 24 maggio 2012 (udienza 17 aprile 2012), n. 19618, in *Cass. pen.*, 2013, p. 1523 ss.

Cass. pen., Sez. II, 15 dicembre 2010, dep. 2008, n. 4178, *Fontana*, in *C.E.D. Cass.*, n. 249207.

Cass. pen., Sez. IV, 13 dicembre 2010, n. 43786, *Cozzini*, in *C.E.D. Cass*., n. 248943.

Cass. pen., Sez. IV, 17 novembre 2010, n. 2622, *Rossini*, in *C.E.D. Cass*., n. 249487.

Cass. pen., Sez. V, 10 marzo 2010, n. 9667, in *Dir. pen. proc*., 2010, p. 1464.

Cass. pen., Sez. V, 14 ottobre 2009, n. 16556, *Virruso*, in *C.E.D. Cassazione*, n. 246954.

Cass. pen., Sez. II, 12 dicembre 2008, n. 47617, *De Luigi*, in *C.E.D. Cass.*, 2008, n. 242304.

Cass. pen., Sez. I, 28 maggio 2008, n. 21366, in *C.E.D. Cass*., n. 240092.

Cass. pen., Sez. I, 21 maggio 2008, n. 31456, *Franzoni*, in *C.E.D. Cass*., n. 259356.

Cass. pen., Sez. VI, 11 dicembre 2007, dep. 2008, n. 15396, *Stizia*, in *C.E.D. Cass.*, n. 239634.

Cass. pen., Sez. I, 16 febbraio 2007, n. 237430, *Pomarici*, in *Cass. pen*., 2008, p. 2956 ss.

Cass. pen., Sez. V, 18 novembre 2004, n. 49376, in *C.E.D. Cass*., 2005, n. 230428.

Cass. pen., Sez. VI, 11 maggio 2004 (udienza 21 gennaio 2004), n. 22397, *Moretti*, in *C.E.D. Cass.*, n. 229396.

Cass. pen., Sez. V, 18 marzo 2004, n. 22818, in *C.E.D. Cass.*, 2004, n. 228818.

Cass. pen., Sez. V, 2 maggio 2002, n. 16130, in *Foro It*., 2002, pt. 2, 635

Cass. pen., Sez. III, 12 febbraio 2002, n. 13641, *Pedron*, in *Cass. pen*., 2003, p. 970 ss.

Cass. pen., Sez. IV, 16 marzo 2000, n. 7063, *Viskovic*, in *C.E.D. Cass*., n. 217688.

Cass. pen., Sez. VI, 4 ottobre 1999, n. 3067, *Piersanti*, in *C.E.D. Cass*., n. 214945.

Cass. pen., Sez. VI, 4 ottobre 1999, n. 3065, in *C.E.D. Cass*., n. 214942.

Cass. pen., Sez. VI, 6 ottobre 1998, n. 2882, *Calcaterra*, in *C.E.D. Cass.*, 1998, n. 212678.

Cass., Sez. VI, 5 febbraio 1998, n. 7162, in *Cass. pen.*, 1999, n. 2137.

Cass. pen., Sez. VI, 16 maggio 1997, n. 1972, *Pacini Battaglia*, in *C.E.D. Cass.*, n. 210045.

Cass. pen., Sez. VI, 7 aprile 1997, n. 1506, *Iannini*, in *C.E.D. Cass*., n. 207591.

Cass., Sez. VI, 12 maggio 1995, n. 9320, in *Cass. pen.*, 1995, 3387.

Trib. Modena, ord. 28 settembre 2016, in *Giur. pen. web*, n. 10, 2016.

Trib. Torino, ord. 7 febbraio 2000.

Trib, di Milano, sez. G.I.P., sentenza 18 giugno 2015, proced. n. 49494/2014 R.G.N.R.

Bundesverfassungsgericht, 27 febbraio 2008, BVerGE 120, 274 ss.

Corte EDU, sez. I, sent. 23 febbraio 2016, ricorso n. 28819/2012, *Capriotti c. Italia.*

Corte EDU, Grande Camera, sent. 4 dicembre 2015, *Zakhrov c. Russia*.

Corte EDU, Grande Camera, 14 settembre 2010, n. 38224, *Sanoma Uitgevers B.V. c. Paesi Bassi*, in *Cass. pen*., 2011.

Corte EDU 18 maggio 2010, *Kennedy contro Regno Unito*.

Corte EDU, 31 maggio 2005, *Vetter contro Francia*.

RINGRAZIAMENTI

Ringrazio il Prof. Moscarini, per la fiducia accordatami e per essere stato un eccellente esempio di costanza, professionalità e dedizione nello studio di questa materia.
Un sentito ringraziamento al Dott. Rubera, per essere diventato il mio punto di riferimento, ma, soprattutto, per la vivacità e l'acutezza dei suoi spunti di riflessione, che sono stati il punto di partenza di questa trattazione.
Un pensiero speciale a Marco e ai miei genitori, che hanno condiviso con me sacrifici e soddisfazioni. Alla mia super nonna, con affetto incondizionato.
A Nico, per esserci sempre stato.
Alle mie amiche di sempre e a quelle che hanno reso questi cinque anni meravigliosi.