

Giuseppe Corasaniti

**LE INTERCETTAZIONI
“UBIQUITARIE” E DIGITALI TRA
GARANZIA DI RISERVATEZZA,
ESIGENZE DI SICUREZZA
COLLETTIVA E DI FUNZIONALITÀ
DEL SISTEMA DELLE PROVE
DIGITALI**

Estratto



Milano • Giuffrè Editore

CASSAZIONE
SEZ. VI PENALE,
6 APRILE 2016
N. 13884 (ORD.)

PRESIDENTE: CARCANO

RELATORE: FIDELBO

• Intercettazioni • Intercettazioni informatiche • Intercettazioni fra presenti • Limiti di utilizzabilità • Programmi informatici di captazione di informazioni • Ammissibilità • Questioni da rimettersi alle Sezioni Unite

Vanno rimesse alle Sezioni Unite penali della Corte di Cassazione le questioni se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'istallazione in congegni

elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi ove deve avvenire la relativa captazione; se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, cod. proc. pen.; e se possa comunque prescindere da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata.

RITENUTO IN FATTO. — 1. Con l'ordinanza indicata in epigrafe il Tribunale di Palermo, in funzione di giudice del riesame, ha confermato il provvedimento del 19 dicembre 2015 con cui il G.i.p. dello stesso Tribunale aveva applicato la misura della custodia cautelare in carcere nei confronti di S.L. in relazione alla partecipazione all'associazione di tipo mafioso denominata "cosa nostra" (capo a) e ad un episodio di tentativo di estorsione aggravata ai danni di A.F., titolare della ditta di costruzioni "E.S.", impegnata nella ristrutturazione di un immobile (capo c).

I giudici del riesame hanno ritenuto sussistenti i gravi indizi di colpevolezza a carico dell'indagato sulla base di una serie di intercettazioni, anche ambientali, e delle dichiarazioni accusatorie di due collaboratori di giustizia, C.F. e d.G.D., dalle quali è emerso che l'indagato, molto vicino a C.P. — divenuto reggente del mandamento di Porta Nuova dopo l'arresto di L.P.T. —, si occupava della gestione delle estorsioni e del traffico di stupefacenti, spesso facendo da intermediario tra lo stesso C. e T.M., moglie del L.P..

Per quanto riguarda l'altro reato, il Tribunale, dopo avere dichiarato l'inutilizzabilità delle intercettazioni effettuate mediante apparecchio body phone, perché in uso a persona diversa rispetto a quella indicata nel decreto, ha tuttavia ritenuto sussistenti gli elementi indiziari in merito al concorso dello S. nell'estorsione gestita dal coindagato G.F.P., giudicato separatamente, ai danni di A.F..

2. L'avvocato Di Marco Maurizio, nell'interesse dell'indagato, ha proposto ricorso per cassazione, deducendo un unico articolato motivo.

L'ordinanza impugnata viene innanzitutto censurata per vizio di motivazione ed erronea applicazione dell'art. 273 cod. proc. pen. con riferimento alla ritenuta sussistenza dei gravi indizi di colpevolezza in ordine al reato associativo, desunti unicamente in base ai risultati delle intercettazioni telefoniche e ambientali, peraltro non suffragate dalle dichiarazioni dei collaboratori di giustizia.

Inoltre, viene dedotta l'illegittimità del decreto n. 315/14, con cui il G.i.p. ha autorizzato "le operazioni di intercettazione di tipo ambientale tra presenti che avverranno nei luoghi in cui si trova il dispositivo elettronico in uso a L.P.T.", nonché l'inutilizzabilità dei risultati relativi a tali captazioni per violazione degli artt. 15 Cost., 8 CEDU, 266, comma 2, e 271 cod. proc. pen. In particolare, il ricorrente dopo aver premesso che l'intercettazione è avvenuta per mezzo di un "virus auto-istallante" attivato su un apparecchio elettronico portatile in uso a L.P.T., ovunque lo stesso si trovasse, ha rilevato come nella specie sia stato eluso il divieto posto dall'art. 266, comma 2, cod. proc. pen. di effettuare intercettazioni all'interno di abitazioni private, a meno che all'interno di esse non si stia svolgendo un'attività criminosa, dal momento che la captazione di conversazioni sarebbe avvenuta anche all'interno dell'abitazione di T.M., coniuge di L.P.T.. A questo proposito nel ricorso si sottolinea come lo stesso G.i.p. avesse respinto un'ulteriore richiesta di autorizzazione alla ripresa audio-video all'interno dell'abitazione di L.P., ritenendola non consentita.

Sotto un diverso profilo, l'intercettazione del dispositivo elettronico portatile sarebbe stata autorizzata in violazione degli artt. 15 Cost. e 8 CEDU in quanto non risulta siano stati indicati i luoghi in cui tale captazione doveva essere effettuata, aggirando, anche in questo caso, i limiti posti dall'art. 266, comma 2, cod. proc. pen.: nel ricorso si sostiene che l'articolo da ultimo citato, attuazione dell'art. 15 Cost., non consente un'applicazione talmente ampia da legittimare forme di intercettazioni, come quella in questione, in grado di seguire il soggetto "ovunque si sposti", in quanto l'intercettazione ambientale per essere legittima deve avvenire in luoghi "ben circoscritti e individuati ab origine" nel decreto autorizzativo. Nella specie, invece, le intercettazioni non sono state soggette ad alcuna restrizione spaziale con la conseguenza che i relativi risultati devono ritenersi inutilizzabili.

Sotto un ulteriore aspetto si evidenzia un vizio di motivazione con riferimento al riconosciuto ruolo di intermediario dello S. tra Sc.Ag. e L.P.T., desunto da alcune intercettazioni telefoniche che però sono ritenute del tutto inidonee a giustificare la ricostruzione contenuta nell'ordinanza.

In relazione alle dichiarazioni rese dai due collaboratori C.F. e G.D., il ricorrente rileva la mancanza di elementi da cui desumere l'intraneità dello S. nell'associazione mafiosa.

Di natura neutra anche le altre intercettazioni, non in grado di giustificare la ritenuta sussistenza di gravi indizi in ordine alla partecipazione all'associazione, ma semmai di consentire di ipotizzare il meno grave reato di favoreggiamento personale.

Con riferimento al reato di tentata estorsione, si contesta la motivazione dell'ordinanza che ha riconosciuto la sussistenza dei gravi indizi in ordine alla partecipazione dello S. solo per aver accompagnato G.F.P. in una trattativa riguardante il pagamento del "pizzo".

CONSIDERATO IN DIRITTO. — 1. Deve rilevarsi che l'ordinanza impugnata desume la sussistenza dei gravi indizi di colpevolezza a carico dello S. per il reato associativo soprattutto in base ai risultati delle intercettazioni, tra cui quelle effettuate sul dispositivo elettronico in uso a L.P.T. tramite l'installazione del virus auto-istallante; le dichiarazioni dei due collaboratori

di giustizia, C.F. e G.D., sono considerate dagli stessi giudici del riesame quali elementi indiziari non dotati di autonoma consistenza, ma in grado semmai di completare il quadro indiziario emergente dall'attività investigativa, che si è appunto concretizzata nell'attività di intercettazione.

Ciò premesso acquista rilevanza prioritaria la questione posta nel ricorso, riguardante la legittimità delle intercettazioni disposte attraverso l'installazione di virus informatici attivati su computer o smartphone e i limiti di utilizzabilità di tali modalità di captazione. Infatti, se fossero fondate le censure che il ricorso muove alla ritenuta utilizzabilità delle intercettazioni eseguite sul dispositivo elettronico in uso a L.P.T. potrebbe rendersi necessario, mediante la c.d. prova di resistenza, verificare se i residui elementi probatori agli atti siano ancora in grado di fondare un giudizio di gravità del quadro indiziario a carico dello S. per la sua partecipazione all'associazione mafiosa.

2. La tesi sostenuta dal ricorrente trova riscontro in una recente sentenza di questa Corte, in un caso analogo a quello in esame, relativo proprio a una intercettazione eseguita tramite un programma spia installato su un dispositivo elettronico portatile (Sez. 6, n. 27100 del 26/05/2015, Musumeci).

In questa decisione la Corte di cassazione ha sostenuto che l'intercettazione da remoto delle conversazioni tra presenti con l'attivazione, tramite il c.d. agente intrusore informatico, del microfono di un apparecchio telefonico smartphone, dia luogo ad una intercettazione ambientale, da ritenere legittima solo se il relativo decreto autorizzativo individui con precisione i luoghi in cui eseguire tale attività captativa. In questi casi non si tratterebbe di "una semplice modalità attuativa del mezzo di ricerca della prova", ma di una tecnica di captazione con specifiche peculiarità in grado di attribuire maggiore potenzialità all'intercettazione, dal momento che consente la possibilità di "captare conversazioni tra presenti non solo in una pluralità di luoghi, a seconda degli spostamenti del soggetto, ma... senza limitazione di luogo". Ed è questa caratteristica che, secondo la sentenza, costituisce il "fulcro problematico della questione", in quanto si assume che non è giuridicamente ammissibile una intercettazione ambientale che avvenga "ovunque". Una corretta lettura delle implicazioni derivanti dall'art. 15 Cost. impedisce di riconoscere all'art. 266, comma 2, cod. proc. pen. una "latitudine operativa così ampia da ricomprendere intercettazioni ambientali effettuate in qualunque luogo": dal principio costituzionale sulla inviolabilità della libertà e della segretezza di ogni forma di comunicazione deriva, secondo la decisione in esame, che le norme sulle intercettazioni, soprattutto quelle tra presenti, siano di stretta interpretazione, sicché deve escludersi che possa attribuirsi all'art. 266, comma 2, cit. "una portata applicativa così ampia da includere la possibilità di una captazione esperibile ovunque il soggetto si sposti". L'unica interpretazione compatibile con la Costituzione è quella che consente l'intercettazione ambientale purché sia autorizzata con riferimento a luoghi individuati ab origine e ben circoscritti, con la conseguenza che la mancanza nel decreto autorizzativo di tali indicazioni determina l'illegittimità del provvedimento e quindi l'inutilizzabilità delle captazioni tra presenti.

3. Nella specie il decreto n. 315/2014, oggetto delle censure da parte del ricorrente, è stato disposto nell'ambito del diverso procedimento n. 762/2012 nei confronti di D.A. ed altri, sospettati di appartenenza a “cosa nostra”, in particolare alla famiglia mafiosa del Borgo Vecchio, e riguarda l'intercettazione di un dispositivo elettronico non meglio specificato — comunque riferibile ad un personal computer, ovvero ad un tablet o ad uno smartphone — in uso a L.P.T., personaggio ritenuto ai vertici dell'organizzazione dopo l'arresto di D.A.; dal provvedimento risulta che sono state autorizzate “operazioni di intercettazione di tipo ambientale delle conversazioni tra presenti che avverranno nei luoghi in cui si trova il dispositivo elettronico in uso a L.P.T.” e nella parte motiva viene precisato che si intende intercettare non il flusso telematico — peraltro già sottoposto a controllo — bensì le conversazioni tra L.P. e gli eventuali altri soggetti presenti nel luogo in cui sia “ubicato in quel momento l'apparecchio portatile”. Sebbene il decreto non appaia del tutto esplicito sulle modalità tecniche dell'intercettazione, risulta evidente dalla lettura complessiva del provvedimento che è stato autorizzato il ricorso alla tecnica del virus informatico applicato al dispositivo elettronico. Più precisamente, attraverso l'installazione da remoto di un captatore informatico, ossia di un software collocato all'interno del dispositivo elettronico, è stata autorizzata una vera e propria intercettazione ambientale attraverso il controllo occulto del microfono che si trasforma in una “cimice informatica”.

Nessuna indicazione specifica è stata fatta con riguardo ai luoghi — ad eccezione dell'abitazione privata di L.P. per respingere la richiesta di video riprese, non effettuabili nel domicilio —, ma solo un riferimento generico ai luoghi in cui si trova il dispositivo elettronico. Né può ritenersi che il riferimento contenuto nel decreto alla “stanza in cui è ubicato in quel momento l'apparecchio portatile” costituisca l'indicazione del limite spaziale in cui avrebbe dovuto operare la captazione, in quanto si tratta di una semplice specificazione che è preceduta dall'indicazione secondo cui l'intercettazione ambientale avverrà all'interno “dei luoghi in cui si trova il personal computer e/o il tablet e/o lo smartphone in uso allo stesso L.P.”, il cui significato non sembra dare adito a dubbi, nel senso di autorizzare l'intercettazione “ovunque” si trovi il dispositivo elettronico.

Ebbene, in base alla citata sentenza n. 27100/2015 di questa Corte, la mancanza di ogni indicazione circa i luoghi interessati dall'intercettazione o meglio la mancanza di limitazioni spaziali alle captazioni ambientali determinerebbe l'illegittimità del decreto autorizzativo e l'inutilizzabilità delle conversazioni captate.

4. In via preliminare deve osservarsi che con riferimento alla tecnica dell'agente intrusore la pretesa di indicare con precisione e anticipatamente i luoghi interessati dall'attività captativa è incompatibile con questo tipo di intercettazione, che per ragioni tecniche prescinde dal riferimento al luogo, in quanto è collegata al dispositivo elettronico, sia esso smartphone o tablet ovvero computer portatile, sicché l'attività di captazione segue tutti gli spostamenti nello spazio dell'utilizzatore. Ovviamente questo comporta l'oggettiva impossibilità per il giudice di conoscere preventivamente gli spostamenti della persona che ha in uso il dispositivo

elettronico sottoposto ad intercettazione e, quindi, di non poter dare indicazioni sui luoghi.

Occorre quindi accertare se la disciplina sulle intercettazioni consente di poter prescindere dall'indicazione del luogo ovvero se, come ritenuto dalla sentenza suindicata, l'omessa indicazione determina l'illegittimità del decreto o quanto meno l'inutilizzabilità dei risultati dell'intercettazione.

4.1. Questo tipo di intercettazione, nonostante le peculiari caratteristiche tecniche, può essere ricompresa nell'ambito di quelle c.d. ambientali: si tratta, infatti, di una captazione occulta e contestuale di colloqui tra due o più persone attuata da un soggetto estraneo mediante uno strumento tecnico di percezione in grado di vanificare le cautele poste a protezione del carattere riservato di tali comunicazioni, che però non avvengono tramite telefono o altre forme di telecomunicazioni; in questo caso, il dispositivo elettronico (ad esempio uno smartphone) rappresenta solo il mezzo attraverso cui viene posizionato, da remoto, l'intrusore informatico che funge da microspia e consente l'ascolto delle conversazioni "tra presenti" al soggetto captante, estraneo alla conversazione e che opera in modo clandestino.

Riconosciuta la collocabilità di tali tecniche di intercettazione nell'ambito della disciplina dell'art. 266, comma 2, cod. proc. pen., si deve rilevare che per l'intercettazione tra presenti il riferimento al luogo acquista rilievo solo quando l'operazione di captazione deve avvenire in abitazioni o luoghi privati. Infatti, questa Corte ha espressamente sostenuto che nelle intercettazioni di comunicazioni tra presenti è richiesta l'indicazione dell'ambiente nel quale deve avvenire l'operazione solo quando si tratti di abitazioni o luoghi privati (Sez. 6, n. 3541 del 05/11/1999, Bembì; Sez. 1, n. 11506 del 25/02/2009, Molè), per i quali l'art. 266, comma 2, cod. proc. pen. consente la captazione in ambiente solo se vi è fondato motivo di ritenere che sia in atto un'attività criminosa. L'inviolabilità del domicilio e in genere dei luoghi di privata dimora prevista dall'art. 14 Cost. ha imposto al legislatore di innalzare il grado di tutela di questi luoghi, prevedendo appunto l'ulteriore presupposto che vi sia un'attività criminosa in corso. È solo in questo caso che nel decreto acquista effettivo rilievo l'indicazione dei luoghi, dal momento che il giudice deve motivare in ordine all'attività criminosa in atto.

4.2. Peraltro, la giurisprudenza considera legittime le intercettazioni tra presenti in cui, nel corso dell'esecuzione delle operazioni, intervenga una variazione dei luoghi in cui l'attività di captazione deve svolgersi: in tali ipotesi l'utilizzabilità delle conversazioni captate viene giustificata purché il luogo "diverso" rientri nella specificità dell'ambiente oggetto dell'intercettazione autorizzata (così, Sez. 6, n. 15396 del 11/12/2007, Sitzia; Sez. 5, n. 5956, del 06/10/2011, Ciancitto; Sez. 2, n. 4178 del 15/12/2010, Fontana; Sez. 2, n. 17894 del 08/04/2014, Alvaro).

In altre parole, si vuole sottolineare come nell'intercettazione tra presenti di tipo "tradizionale" il riferimento al luogo rileva limitatamente e in relazione alla motivazione del decreto, in cui il giudice deve indicare le situazioni ambientali oggetto della captazione e ciò è funzionale alle

modalità esecutive dell'intercettazione, che avviene per mezzo della collocazione fisica di microspie.

Un'esigenza di questo tipo è del tutto estranea all'intercettazione per mezzo del c.d. virus informatico, in quanto la caratteristica tecnica di tale modalità di captazione prescinde dal riferimento al luogo, trattandosi di una intercettazione ambientale per sua natura itinerante. In realtà, ciò che rileva nelle intercettazioni di questo genere è che il decreto autorizzativo sia adeguatamente motivato per giustificare le ragioni per le quali si ritiene debba utilizzarsi la metodica dell'installazione da remoto, consentendo così una captazione dinamica.

4.3. Invero, sebbene debba riconoscersi la formidabile invadenza di questo genere di intercettazioni, allo stesso modo si può rilevare che il principio secondo cui il decreto deve individuare con precisione i luoghi in cui dovrà essere eseguita l'intercettazione delle comunicazioni tra presenti non solo non è desumibile dalla legge, ma, come si è visto, non risulta essere stato mai affermato dalla giurisprudenza e, inoltre, non sembra costituire un requisito significativo funzionale alla tutela dei diritti in gioco (artt. 14, 15 Cost. e 8 Cedu), dal momento che la stessa Corte Europea dei diritti dell'uomo non ne fa menzione.

Secondo la giurisprudenza di Strasburgo le garanzie minime che la legge nazionale deve apprestare nella materia delle intercettazioni riguardano la predeterminazione della tipologia delle comunicazioni oggetto di intercettazione, la ricognizione dei reati che giustificano tale mezzo di intrusione nella privacy, l'attribuzione ad un organo indipendente della competenza ad autorizzare le intercettazioni con la previsione del controllo del giudice, la definizione delle categorie di persone che possono essere interessate, i limiti di durata delle intercettazioni, la procedura da osservare per l'esame, l'utilizzazione e la conservazione dei risultati ottenuti, la individuazione dei casi in cui le registrazioni devono essere distrutte (cfr., Corte EDU, 31 maggio 2005, Vetter c. Francia; Corte EDU, 18 maggio 2010, Kennedy c. Regno Unito). Nessun riferimento alla indicazione del luogo della captazione.

5. Il problema delle intercettazioni per mezzo del c.d. "captatore informatico" riguarda esclusivamente il domicilio e i luoghi di privata dimora considerati dall'art. 614 cod. pen. espressamente richiamato dall'art. 266, comma 2, cod. proc. pen. Infatti, il carattere itinerante della captazione può consentire l'acquisizione di registrazioni di conversazioni avvenute nel domicilio o comunque in ambienti privati, che neppure l'espressa esclusione di tali luoghi nel decreto di autorizzazione può di fatto impedire, in quanto una volta installato il "virus informatico" la captazione audio avviene seguendo indistintamente tutti gli spostamenti del possessore del dispositivo elettronico.

In questi casi, se si ammette la possibilità di utilizzare l'intercettazione per virus informatico, in mancanza della possibilità concreta di sospensione o interruzione della registrazione, il controllo non potrà che essere successivo e riguardare il regime dell'inutilizzabilità delle conversazioni captate in uno dei luoghi indicati dall'art. 614 cod. pen.. È evidente che la fase dello stralcio di cui all'art. 268, comma 6, cod. proc. pen. potrebbe

costituire il primo momento in cui verificare che le intercettazioni non abbiano riguardato colloqui effettuati nel domicilio: il giudice, d'ufficio ovvero su indicazione delle parti, dovrà immediatamente stralciare le registrazioni delle conversazioni avvenute nei luoghi indicati dall'art. 614 cod. pen., trattandosi di intercettazione non consentita e quindi inutilizzabile; inoltre, al di fuori di questa fase sarà sempre consentito eccepire l'inutilizzabilità delle conversazioni intercettate in un luogo privato. In ogni caso, deve riconoscersi che non sempre sarà immediatamente evidente che si tratti di intercettazione eseguita in uno dei luoghi indicati dall'art. 614 cod. pen., sicché appare essenziale l'apporto della difesa nell'indicare le conversazioni inutilizzabili.

I maggiori problemi riguardano l'uso delle intercettazioni con virus informatico nel procedimento de libertate, soprattutto considerando che il giudice può pronunciarsi sulla misura cautelare richiesta sulla base del solo "brogliaccio". In questa ipotesi è difficile che dal brogliaccio emerga che un'intercettazione è avvenuta in un luogo privato, sicché diventa fondamentale che la difesa sia messa in condizione di poter contraddire sul punto: a questi fini appare rilevante la sentenza n. 36 del 2008 della Corte costituzionale che, dichiarando la parziale illegittimità dell'art. 268 cod. proc. pen., ha consentito che dopo la notificazione o l'esecuzione dell'ordinanza che dispone una misura cautelare personale il difensore possa ottenere la trasposizione su nastro magnetico delle registrazioni di conversazioni intercettate e utilizzate ai fini dell'adozione della misura, anche se non depositate.

6. Nel procedimento in oggetto una serie di colloqui, utilizzati dal Tribunale per sostenere la sussistenza dei gravi indizi di colpevolezza dello S. (v., intercettazioni del 12.7.2014 e del 23.7.2014), risultano essere stati intercettati nell'abitazione privata in uso a T.M., moglie di L.. Tuttavia, deve osservarsi che l'intercettazione è stata disposta ai sensi dell'art. 13 del d.l. 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, per cui non si porrebbe neppure il problema dei luoghi di privata dimora, in quanto, come è noto, l'intercettazione tra presenti che sia disposta in un procedimento relativo a un delitto di criminalità organizzata è consentita anche se non vi è motivo di ritenere che nei luoghi indicati dall'art. 614 cod. pen. si stia svolgendo l'attività criminosa.

È evidente che, in presenza di intercettazioni relative a procedimenti di criminalità organizzata, l'indicazione del luogo risulta ancor più irrilevante, anche in rapporto all'utilizzo della tecnica del virus informatico. In questi casi, gli aspetti problematici delle intercettazioni per agente intrusore che si sono evidenziati nemmeno si pongono, dal momento che le captazioni delle conversazioni nei luoghi di privata dimora non sono soggette ad alcuna disciplina in deroga rispetto agli altri luoghi.

Tuttavia, deve rilevarsi che la più volte richiamata sentenza n. 27100 del 26/05/2015, ric. Musumeci, aveva anch'essa ad oggetto un'intercettazione disposta nell'ambito di un procedimento di criminalità organizzata, ma non sembra aver attribuito alcun rilievo a tale circostanza, ritenendo comunque indispensabile che il decreto autorizzativo debba contenere una precisa individuazione dei luoghi in cui procedere ad intercettazione ambientale, mettendo in diretta correlazione tale requisito con la tutela offerta dall'art.

15 Cost. e così trasformando in requisito dell'autorizzazione quella che sembrerebbe essere una modalità di attuazione dell'intercettazione.

7. Per le ragioni sopra esposte, questo Collegio non ritiene di poter condividere le radicali conclusioni cui perviene la sentenza n. 27100/2015 citata.

Considerata la delicatezza della materia, in cui il ricorso a strumenti di sofisticata tecnica informatica, di così formidabile invadenza nella sfera della privacy e nello stesso tempo di applicazione tendenzialmente semplice, può determinare, da un lato, la compromissione di diritti costituzionali, dall'altro, assicurare una maggiore capacità investigativa finalizzata alla repressione di gravi reati, si ritiene che la questione debba essere rimessa alle Sezioni Unite, per evitare potenziali contrasti di giurisprudenza su un tema di tale rilevanza, anche tenuto conto della ormai diffusa utilizzazione delle tecniche di intercettazione con il c.d. agente intrusore.

In particolare, le questioni che possono derivare da un possibile contrasto giurisprudenziale possono essere così sintetizzate:

— se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi ove deve avvenire la relativa captazione;

— se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, cod. proc. pen.;

— se possa comunque prescindere da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata.

8. In conclusione, visto l'art. 618 cod. proc. pen., rimette il ricorso alle Sezioni Unite.

P.Q.M. — Rimette il ricorso alle Sezioni unite.

*LE INTERCETTAZIONI
“UBIQUITARIE” E DIGITALI
TRA GARANZIA DI
RISERVATEZZA, ESIGENZE
DI SICUREZZA COLLETTIVA
E DI FUNZIONALITÀ DEL
SISTEMA DELLE PROVE
DIGITALI*

tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in

La VI sezione penale della Cassazione ha chiesto che venga sottoposta alle Sezioni Unite la questione se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un “virus” informatico (Trojan) debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi ove deve avvenire la relativa captazione, se, in mancanza di

concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, cod. proc. pen., se possa comunque prescindere da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata.

Il tema offre numerosi spunti di riflessione.

1. LE INTERCETTAZIONI “UBIQUITARIE” E L’ORIENTAMENTO NEGATIVO.

La questione della legittimità delle intercettazioni “ubiquitarie” cioè delle intercettazioni di contenuti sonori o video operata a distanza con attivazione di programma applicativo per dispositivo mobile si appresta ad essere trattata dalle S.U. della cassazione, e il tema — tanto più nell’attuale contesto — si presenta quanto mai controverso e delicato.

Secondo l’orientamento più recente della Corte di cassazione (Sez. 6, sentenza n. 27100 26 maggio 2015) la tematica dell’intercettazione di contenuti digitali si articola su due versanti distinti, che si riconnetterebbero in particolare a precise peculiarità tecniche che si riferiscono solo alcune intercettazioni: l’attivazione, da remoto, del microfono e l’attivazione, sempre da remoto, della telecamera. Come si dirà tali profili problematici appaiono circoscritti e distinti.

Muovendo dalla prima delle peculiarità tecniche — osserva la Corte — occorre osservare che l’attivazione del microfono (da remoto) dà luogo di fatto ad un’intercettazione ambientale, onde occorre interrogarsi sulla legittimità della stessa”. Secondo la Corte, infatti, “*non sembra potersi dubitare che l’art. 266 c.p.p., comma 2, nel contemplare l’intercettazione di comunicazioni tra presenti, si riferisca alla captazione di conversazioni che avvengano in un determinato luogo e non ovunque*”. Si precisa allora come “una corretta ermeneutica della norma di cui all’art. 15 Cost. osta infatti all’attribuzione al disposto dell’art. 266 c.p.p., comma 2 di una latitudine operativa così ampia da ricomprendere intercettazioni ambientali effettuate in qualunque luogo. La norma costituzionale pone, infatti, secondo la Corte il fondamentale principio secondo il quale la libertà e la segretezza delle comunicazioni sono inviolabili, ammettendo una limitazione soltanto per atto motivato dell’autorità giudiziaria e con le garanzie stabilite dalla legge.

Ne deriva che le norme che prevedono la possibilità di intercettare comunicazioni “tra presenti” sarebbero di stretta interpretazione, ragion per cui non può considerarsi giuridicamente corretto attribuire alla

* In data 28 aprile 2016 le S.U., con sentenza in corso di pubblicazione al momento della stampa, pronunciandosi sulla questione se — 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 — sia consentita l’intercettazione di conversazioni o comunicazioni tra presenti, mediante l’installazione di un “captatore informatico” in dispositivi elettronici portatili (ad es., *personal computer, tablet, smartphone*

ecc.), hanno affermato come l’uso di tale strumento sia consentito, limitatamente a procedimenti relativi a delitti di criminalità organizzata, anche terroristica (a norma dell’art. 13 d.l. n. 152 del 1991), intendendosi per tali quelli elencati nell’art. 51, commi 3-bis e 3-quater, cod. proc. pen., nonché quelli comunque facenti capo a un’associazione per delinquere, con esclusione del mero concorso di persone nel reato.

norma codicistica una portata applicativa così ampia da includere la possibilità di una captazione esperibile ovunque il soggetto si sposti. Viceversa, l'unica opzione interpretativa compatibile con il dettato costituzionale è quella *secondo la quale l'intercettazione ambientale deve avvenire in luoghi ben circoscritti e individuati ab origine e non in qualunque luogo si trovi il soggetto*¹.

Nella stessa prospettiva, si ammette che, una volta autorizzata la captazione delle conversazioni in un determinato luogo, l'attività deve ritenersi consentita anche nelle pertinenze, senza necessità di ulteriore specifica autorizzazione ma ciò proprio sulla base del presupposto che la pertinenza non possa considerarsi luogo diverso dall'abitazione principale, all'interno del quale l'intercettazione sia stata autorizzata (Cass., Sez. 2, n. 4178/11 del 15-12-2010). Ove la tecnica utilizzata consente, attraverso l'attivazione del microfono del telefono cellulare, la captazione di comunicazioni in qualsiasi luogo si rechi il soggetto, portando con sé l'apparecchio, non sarebbe perciò — secondo la Corte — giuridicamente ammissibile. Non si tratta pertanto, in tale prospettiva, di una semplice modalità attuativa del mezzo di ricerca della prova, costituito dalle intercettazioni. Si tratterebbe invece di una tecnica di captazione che presenta delle specifiche peculiarità e che aggiunge un *quid pluris*, rispetto alle ordinarie potenzialità dell'intercettazione, costituito, per l'appunto, dalla possibilità di captare conversazioni tra presenti non solo in una pluralità di luoghi, a seconda degli spostamenti del soggetto, ma — ciò che costituisce il fulcro problematico della questione — senza limitazione di luogo, in contrasto con il precetto costituzionale di cui all'art. 15 Cost.

Quindi, nella prospettiva della Corte il decreto autorizzativo del giudice dovrà (preventivamente) individuare, con precisione, i luoghi nei quali dovrà essere espletata l'intercettazione delle comunicazioni tra presenti, *non essendo ammissibile un'indicazione indeterminata o addirittura l'assenza di ogni indicazione, al riguardo*. Quanto alla attivazione della videocamera del telefono cellulare e quindi l'effettuazione di videoriprese la Corte ha richiamato il principio (espresso da Sez. U. 28-3-2006, n. 26795) per cui le videoregistrazioni in luoghi pubblici o aperti o esposti al pubblico, non effettuate nell'ambito del procedimento penale, vanno incluse nella categoria dei documenti, ex art. 234 cod. proc. pen.².

¹ Secondo la Corte, infatti, in giurisprudenza, si ammetterebbe la variazione dei luoghi in cui deve svolgersi la captazione solo se rientrando nella specificità dell'ambiente oggetto dell'intercettazione autorizzata (Cass., Sez. 6, n. 15396 dell'11-12-2007, relativa ad una fattispecie in cui l'autorizzazione dell'intercettazione ambientale aveva ad oggetto la sala colloqui della Casa circondariale in cui era ristretto l'imputato e le operazioni di captazione erano proseguite presso la sala colloqui della Casa circondariale in cui lo stesso era stato successivamente trasferito).

² Secondo la Corte, che appunto si richiama alla teoria "documentale" tali registrazioni, se vengono invece effettuate dalla p.g., anche d'iniziativa, vanno incluse nella categoria delle prove atipiche, soggette alla disciplina dettata dall'art. 189 cod. proc. pen.. Ma esse non possono essere espletate ovunque, perché le videoregistrazioni effettuate in ambito domiciliare, ai fini del procedimento penale, sono acquisite illecitamente e sono perciò inutilizzabili, anche se la tutela costituzionale del domicilio va limitata ai luoghi con i quali la persona abbia un rapporto stabile, sicché, quando si tratta di

2. INTERCETTAZIONI “AMBIENTALI” E INTERCETTAZIONI “TRA PRESENTI” TRA REALTÀ E PRASSI OPERATIVE.

Le intercettazioni di conversazioni tra presenti sono espressamente previste, accanto a quella di conversazioni telefoniche, dal secondo comma dell'art. 266 cod. proc. pen., secondo cui le intercettazioni di tal genere da eseguirsi in una abitazione o in altro luogo di privata dimora o nelle appartenenze di essi (luoghi espressamente elencati nell'art. 614 c.p., richiamato dall'art. 266 comma 2 c.p.p.), sono consentite solo se vi sia il fondato sospetto che ivi si stia svolgendo l'attività criminosa. Tale condizione — è bene sottolinearlo — *non è invece richiesta quando l'intercettazione riguarda un procedimento per delitto di criminalità organizzata* (art. 13, comma 1 seconda parte, d.l. 13 maggio 1991 n. 153 conv. in l. 12 luglio 1991, n. 203).

Tale assetto normativo è stato ritenuto, dalla giurisprudenza di legittimità, del tutto coerente con la tutela dei valori costituzionali (Sez. VI, 20 febbraio 1991, n. 660).

Tali disposizioni sono state di seguito estese ai reati di terrorismo³ rispetto ai quali la tematica delle intercettazioni “ubiquitarie” perde qualsiasi significato concreto a causa della specificità delle previsioni autorizzatorie in ragione della gravità dei reati ipotizzabili e dell'esigenza di prevalenza di garanzie di sicurezza rispetto ad una astratta ed indefinita tutela del “domicilio” della persona intercettata. In realtà l'uso della terminologia giurisprudenziale, con il suo riferimento all’“ambiente” e non alla persona “presente” contestualmente e coinvolta in contatti investigati potrebbe avere influito non poco sulla coerenza delle scelte giurisprudenziali.

Il “virus”, come ben sa anche il più sprovveduto degli informatici è un *programma creato per distruggere dati e programmi* introducendosi abusivamente nei sistemi operativi, e come dovrebbe sapere il giurista è il programma cui si riferisce l'art. 615-*quiquies* c.p., quindi un programma che ha uno scopo preciso ed illecito, quello di danneggiare “illecitamente” un sistema informatico, le informazioni, i dati e i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione parziale o totale del suo funzionamento. Il virus “trojan (horse)”, che echeggia scenari omerici derivando il suo nome dal mitico “cavallo” ideato da Odisseo non è altro che un programma autoinstallante che consente di acquisire o replicare dati e informazioni trasmettendole all'esterno del sistema informatico, attraverso tale tecnica la sua utilizzazione è una costante della organizzazione delle frodi informatiche

tutelare solo la riservatezza, la prova atipica può essere ammessa con provvedimento motivato dell'autorità giudiziaria. *Vanno dunque tutelate dall'autorità giudiziaria (p.m. o giudice) le riprese visive che, pur non comportando intrusione domiciliare, violino la riservatezza personale (come, ad esempio, le riprese effettuate dalla polizia giudiziaria in un bagno pubblico).*

³ L'estensione è stata operata con il decreto-legge 18 ottobre 2001, n. 374 con-

vertito nella 15 dicembre 2001, n. 438. Il recente decreto in tema di terrorismo internazionale (legge 17 aprile 2015, n. 43 Conversione in legge, con modificazioni, del decreto-legge 18 febbraio 2015, n. 7, recante misure urgenti per il contrasto del terrorismo, anche di matrice internazionale), in tale contesto si è ancora ampliata la possibilità di acquisizione di dati e documenti informatici anche con finalità preventive dei delitti di terrorismo internazionale introducendo l'art. 234-*bis* c.p.

(malware che, introdotto nei computers trasmette password o dati personali all'esterno). La suggestione del termine e la falsa analogia "biologica" rende semplice talora accostare al termine una implicita negatività assoluta, tanto ingiustificata se in rapporto a metodologie ed a controlli (pubblici dato che ovviamente la condotta di intercettazione abusiva svolta abusivamente è addirittura penalmente sanzionata *ex artt.* 617 e *bis* e *quater* del c.p. che sanziona appunto anche più gravemente le intercettazioni telefoniche e informatiche "abusive") che invece si riferiscono ad attività investigative e tecniche del tutto indispensabili entro un contesto propriamente e strettamente governato dal controllo giurisdizionale.

In un quadro di intercettazione telefonica ed ambientale, infatti, le attività operative che inseriscono strumenti o congegni di captazione informativa audio e video non possono che essere concepite se non come assolutamente e strettamente riservate e, soprattutto occultate, in quanto implicitamente la minima rivelazione, anche indiretta della loro esistenza funzionale o spaziale (la presenza di microfoni o congegni di videoregistrazione anche di ridottissime dimensioni) rischia di compromettere totalmente l'indagine, sicché è evidente che la relativa collocazione avviene solitamente non solo in modo riservato, ma talora in modo occulto ai soggetti interessati mediante tecniche varie di carattere "fisico" che oggi sono totalmente bypassate dall'uso e dal governo "esterno" degli apparati informatici eventualmente posseduti od utilizzati, in un contesto nel quale l'ambientazione "informatica" non riproduce solo gli schemi tradizionali della intercettazione vocale "telefonica" — cioè svolta in buona sostanza con una duplicazione controllata del segnale fonico che dell'intercettazione è oggetto diretto — ma svolgono i loro effetti (previamente autorizzati e controllati dal giudice per le indagini preliminari) direttamente sul "sistema" informatico altrui una volta individuato, inserendosi un programma esattamente come una microspia (cioè un dispositivo elettronico "fisico" miniaturizzato, che una volta peraltro era nota con il termine non meno spregiativo della "cimice").

3. INTERCETTAZIONI DIGITALI E "DI FLUSSO" (DIGITALE) DI COMUNICAZIONI.

Come è noto ai sensi dell'art. 266-*bis* c.p.p. (introdotto con la prima legge sui reati informatici, art. 11 legge 23 dicembre 1993 n. 547) nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche "è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi"...⁴. In informatica si definisce "flusso" di comunicazioni *ogni flusso di esecuzione di un programma da parte del processore operato grazie alle strutture di controllo tipiche del linguaggio di programmazione in cui è scritto il codice sorgente del programma stesso*. Ne consegue, come è stato correttamente rilevato⁵ che la problematica sui contenuti digitali rileva in modo

⁴ Cfr. DE FLAMMINEIS V., *Le intercettazioni telematiche*, in *Diritto penale e processo*, 2013, 8, pp. 988-992.

⁵ ORLANDI R., *Questioni attuali in tema di processo penale e informatica*, in *Rivista*

di diritto processuale, 2009, 1, pp. 129-137. Cfr. anche sul tema F. ZACCHÈ F., *L'acquisizione della posta elettronica nel processo penale*, in *Processo penale e Giustizia*, 2013, 4, pp. 9.

assai significativo se è vero che nell'art. 266-bis c.p.p. si parla di "comunicazioni" eseguite con l'impiego di tecnologie informatiche e telematiche, ma che è indubbio che la norma allude (solo) alla intercettazione di tali comunicazioni. Essa sembra quindi apparentemente riferirsi ai soli casi di "captazione" del messaggio eseguibile nel lasso di tempo che separa l'invio dal momento in cui il destinatario ne prende conoscenza.. Secondo tale prospettiva allora, una volta giunto a destinazione, il messaggio non sarebbe più intercettabile, bensì "acquisibile" mediante esibizione spontanea o con le modalità (formali) del sequestro. Le intercettazioni di e-mail suppongono infatti comunicazioni di contenuti scritti, con tempi diversi per l'invio e per l'effettiva ricezione. Perciò si osserva ⁶ se le prime hanno carattere sincronico, le altre sono, per così dire, asincrone. Ne segue allora che l'acquisizione di messaggi e-mail non ancora letti cade sotto l'applicazione dell'art. 266-bis c.p.p. Non così i messaggi già letti che vanno trattati analogamente a lettere già aperte, dissigillate, vale a dire come "documenti informatici" coperti dalla riservatezza che garantisce le informazioni di carattere personale, ma non tali da meritare la più intensa tutela apprestata dagli artt. 266 ss. c.p.p. in attuazione dell'art. 15 Cost.

4. CONTENUTI DIGITALI E PROBLEMI FORMALI.

La giurisprudenza della Corte (Sez. U, Sentenza n. 21 del 13/07/1998) si è dapprima riferita all'acquisizione "formale" e "documentale" dei dati "esterni" della comunicazione (c.d. *"tabulato che in pratica documenta l'intervenuta comunicazione telefonica tra due utenti registrandone le utenze, le celle impegnate la durata e gli elementi che comprovano l'intervenuta comunicazione fonica"*) segnalando come la stampa dei tabulati concernenti il flusso informatico relativo ai dati esterni al contenuto delle comunicazioni telefoniche *costituisce la documentazione, in forma intelligibile, del flusso medesimo*, la relativa acquisizione perciò soggiace

⁶ Sempre Orlandi R. cit. lo stato attuale della normativa processuale italiana in tema di operazioni investigative informatiche sarebbe visibilmente inadeguato. A uno sviluppo tecnologico capace di creare nuove sfide e inediti pericoli sul terreno dei diritti fondamentali non è corrisposta una elaborazione giuridica in grado di proteggere i titolari di quei diritti.

Un tema di assoluta rilevanza, per il diritto penale dell'informatica, è inoltre il compromesso, difficile ma non eludibile, che si dovrà trovare tra tutela dei dati personali e tutela dell'ordine pubblico. Nel nuovo contesto criminale che si avvale del web l'investigazione digitale ha assunto un ruolo essenziale e determinante, in quanto il valore delle informazioni che la polizia giudiziaria può rinvenire, all'interno di un personal computer o attraverso un'intercettazione telematica o anche solo attraverso una semplice navigazione su Internet, è enorme. Tuttavia, si è correttamente osservato, men-

tre nella perquisizione di un appartamento o in una intercettazione telefonica i limiti della giurisdizione nazionale non vengono quasi mai toccati, nel momento stesso in cui oggetto dell'indagine è il dato digitale quasi automaticamente insorge il conflitto tra diverse giurisdizioni, senza neppure arrivare a toccare i possibili problemi che saranno generati dalla sempre maggiore espansione del cloud computing. Nel momento stesso in cui si crea un potenziale conflitto giurisdizionale non è solo rilevante l'aspetto procedurale (rogatorie, convenzioni e accordi internazionali), ma diventano determinanti le differenze giuridiche, politiche, culturali e sociali tra i vari Paesi, in una tematica trasversale come è sicuramente quella della protezione dei dati personali. Così VACIAGO G., *Privacy e tutela dell'ordine pubblico in Europa e negli Stati Uniti: un differente approccio per raggiungere un difficile compromesso*, in *Informatica e diritto*, 2009, 1, pp. 135-150.

alla stessa disciplina delle garanzie di segretezza e libertà delle comunicazioni a mezzo di sistemi informatici di cui alla legge 23 dicembre 1993 n. 547 (che ha introdotto l'art. 266-bis e modificato l'art. 268 cod. proc. pen.), sicché il *divieto di utilizzazione previsto dall'art. 271 cod. proc. pen. è riferibile anche all'acquisizione dei tabulati predetti tutte le volte che avvenga in violazione dell'art. 267, cioè in assenza del prescritto decreto motivato*. In motivazione la Corte ha invero precisato che la legittima acquisizione dei tabulati in parola *può essere disposta nel corso delle indagini preliminari dal pubblico ministero e dal giudice che procede — art. 267 cod. proc. pen. — o dal giudice del dibattimento o di appello, rispettivamente ai sensi degli artt. 507 e 603 cod. proc. pen.*) (v. Corte Cost., sentenze n. 81 del 1993 e 281 del 1998).

A riguardo va segnalato come in passato (Sez. 5, Sentenza n. 10858 del 21/10/1996) la Corte ha persino ammesso la possibilità di intercettazione e di registrazione di conversazioni che si svolgono via radio su bande non protette e per mezzo di un apparecchio ricetrasmittente privo di concessione, le quali non necessitano dell'autorizzazione del giudice e non sarebbero perciò sottoposte al regime previsto per le intercettazioni telefoniche. Ma il problema di fondo è soprattutto dare un significato “tecnico” e non formale alla c.d. “*intercettazione di flusso*” anche alla luce del chiaro disposto dell'art. 234 c.p.p. che consente la piena acquisizione della prova documentale *rappresentativa di fatti*, persone o cose mediante la fotografia, la cinematografia *la fonografia o qualsiasi altro mezzo*.

Peraltro il problema appare duplice, da un lato la telefonia oggi è sostanzialmente mutata con una prevalenza dei c.d. apparati “mobili”, che nell'attuale fase tecnologica altro non sono che apparati “*smart-phone*” cioè sostanzialmente veri e propri computers *dotati di proprio sistema operativo e applicazioni di comunicazione vocale* che rendono sostanzialmente inutile il ricorso a forme di intercettazione telefonica “tradizionale” in quanto le comunicazioni vocali operano su protocolli diversi (*Voice over IP, Voce tramite protocollo Internet o VoIP, tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet o una qualsiasi altra rete dedicata a comunicazione di pacchetto che utilizzi il protocollo IP senza connessione per il trasporto dati*).

Una prima notazione può trarsi allora da Sez. 1, Sentenza n. 4561 del 30/06/1999 che sottolineava come mentre le intercettazioni di conversazioni o comunicazioni effettuate mediante l'uso del telefono, nonché di altre forme di telecomunicazione ovvero di sistemi informatici o *telematici presuppongono l'esistenza di una specifica apparecchiatura o di un particolare sistema da sottoporre a intercettazione*, sicché, per ciascuna operazione di intercettazione, i relativi dati di identificazione devono essere precisati in maniera particolare nei rispettivi decreti autorizzativi, le intercettazioni delle comunicazioni tra presenti, di cui al secondo comma dell'art. 266 cod. proc. pen., per la loro intrinseca natura, non presuppongono, perché siano realizzate, la mediazione di mezzi tecnici, come tali provvisti necessariamente di dati identificativi, *sicché la variazione non dello specifico ambiente per il quale è stata autorizzata l'intercettazione, ma soltanto della diversità del mezzo che lo connota, pur sempre rientrante nella specificità dell'ambiente oggetto dell'intercettazione autorizzata, non è ostativa all'utilizzazione del contenuto delle intercettazioni eseguite sull'uno o sull'altro mezzo di svolgimento delle conversazioni tra presenti*. (Fattispecie peraltro relativa a intercettazione

ambientale autorizzata per una autovettura nella disponibilità dell'indagato ed eseguita invece su diversa autovettura, sempre nella sua disponibilità)⁷.

Peraltro non è estranea all'argomento neppure la questione della intercettazione telefonica "a cornetta sollevata", ossia il casuale ascolto di tale conversazione nel corso di una intercettazione telefonica ritualmente autorizzata. In particolare si discute cioè in tal caso vi sia una prova legittimamente utilizzabile oppure se, al contrario, per la relativa captazione occorra il rispetto delle condizioni poste per le intercettazioni ambientali. Qui in vece è da registrare un netto orientamento nel senso che la registrazione di colloqui fra presenti, intervenuta casualmente, non dipende da una indebita violazione della privacy ma dal comportamento degli interlocutori i quali, lasciando il ricevitore alzato fanno sì che la loro conversazione — altrimenti percepibile solo tramite una intercettazione ambientale — sia invece percepita fonicamente rimanendo scoperta dal punto di vista della segretezza. Considerano dunque il risultato utilizzabile ai fini della applicazione di una misura cautelare, non rientrando nella sfera di operatività degli artt. 15 Cost. e 266-271 c.p.p.⁸.

Il tema della utilizzabilità delle intercettazioni telefoniche si presenta perciò come un tema di particolare delicatezza e di indubbia valenza tecnologica, tanto più perché destinato ad operare in ambiti differenziati, a riferirsi a condotte accertate tra le più varie, a porre, in definitiva con continuità, il problema della prevalenza nei casi concreti di una esigenza protettiva (del soggetto intercettato in certi ambiti domiciliari o dei soggetti che con questi vengono a contatto relazionandosi in modo spontaneo)⁹.

Il tema, questo, che appare particolarmente approfondito dalla dottrina penalistica che si muove, in sostanza, tra percezione della comples-

⁷ Peraltro cfr. anche Sez. 2, Sentenza n. 1831 del 12/03/1998 che precisa come ai fini della individuazione delle condizioni e dei limiti di ammissibilità delle intercettazioni di comunicazioni tra presenti, rientrano nel concetto di privata dimora tutti quei luoghi che, oltre all'abitazione, assolvano alla funzione di proteggere la vita privata e che siano perciò destinati al riposo, all'alimentazione, alle occupazioni professionali e all'attività di svago, tra cui va ricompreso l'abitacolo di una autovettura adibita, di regola, ai trasferimenti da e per il luogo di lavoro e di svago. È pertanto legittima l'intercettazione di colloqui tra presenti che si svolgono all'interno di un'autovettura quando esista il fondato sospetto, che ivi si stia svolgendo l'attività criminosa, da intendersi come prognosi da formulare con giudizio "ex ante" all'atto della emanazione del provvedimento di autorizzazione, giacché in tal caso l'interesse all'inviolabilità del domicilio trova il limite della tutela di interessi generali, anch'essi costituzionalmente garantiti, ravvisabili nell'esigenza di esercitare l'azione penale che, "ex" art. 112 Cost., è obbligatoria.

⁸ Così Sez. 5, 21 ottobre 2003, n. 44714; Sez. 6, 9 gennaio 2003, n. 25682; Sez. 6, 18 marzo 1998, n. 982; Sez. 6, 8 aprile 1994, n. 6633; Sez. 6 4 giugno 1993, n. 9443.

⁹ Cfr. sul punto BARONE L., *L'utilizzabilità delle intercettazioni come corpo di reato*, in *Cassazione penale*, 2015, 4S, pp. 181-185; CHIARELLA P., *Tra diritto di cronaca e privacy (sul filo delle intercettazioni telefoniche e degli internet blog)*, in *Sociologia del diritto*, 2010, 2, pp. 127-143; SPINELLI A., *Videoregistrazioni: tra prove atipiche e deficit di tutela della cassazione*, in *Diritto penale e processo*, 2011, 9, pp. 1129-1136; NEVOLI F., *Intercettazioni informatiche e telematiche: ricorso ad impianti esterni ed obbligo motivazionale del pubblico ministero*, in *Archivio della nuova procedura penale*, 2010, 1, pp. 76-80; GAMBINI R., *La politica di law and order nella disciplina delle intercettazioni telefoniche e dell'ascolto elettronico*, in *Diritto penale e processo*, 2009, 2, pp. 251-257; MAFFEO V., *La riforma in itinere delle intercettazioni, tra tutela della privacy ed esigenze dell'accertamento*, in *Diritto penale e processo*,

sità del panorama tecnologico in evoluzione e proiezione della problematicità di una definizione normativa non solo inadeguata, poiché appunto riferibile ad un contesto ben differente di comunicazioni, prevalentemente foniche, ma ben più delicato ove si consideri che la “registrazione” dei contenuti viene oggi ad inquadrarsi in chiave “multimediale” (cioè aperta ad ogni messaggio testuale, visivo e sonoro, con dettagli e qualità prima inimmaginabili) e che tali contenuti si scambiano e vengono registrati su sistemi informatici.

Ne consegue una più attenta registrazione delle istanze difensive in termini di controllo e di garanzia, che si spinge a verificare in termini funzionali l’acquisizione dei dati e delle informazioni in rapporto all’impianto complessivo e relazionale emergente in concreto sia sul piano del rispetto della legittima acquisizione della fonte di prova (perché tale è in buona sostanza l’intercettazione in ambito processuale), sia in considerazione delle delicate implicazioni che appaiono insistenti nella percezione, sia pur legittima, dei contenuti di relazioni umane, i quali possono e debbono risultare funzionali, anche in termini di coerenza, di significatività nonché di proporzionalità ed adeguatezza, in rapporto ad una ricerca investigativa ben definita nei suoi obiettivi e soprattutto controllata giurisdizionalmente nel suo evolversi e nella sua utilizzabilità processuale. Le prospettive di riforma sono state pressoché costanti in questi ultimi anni, ed esse oscillano tra esasperazione delle garanzie processuali individuali e ricerca di un punto di equilibrio sostanziale.

È ben noto il rischio di vanificare del tutto l’utilizzazione di uno strumento di indagine tanto prezioso quanto efficace, ed è altrettanto noto il problema che un uso eccessivo e sistematico di strumenti informativi di captazione diretta di contenuti informativi produca una mutazione genetica anche sulle indagini penali, per lo più ridotte a mero ordinamento di contenuti intercettati. Si può dire, tuttavia, che alla luce di una corretta analisi della vigente normativa, tale rischio, se pure ciclicamente paventato e più volte sottolineato con (generici) richiami alla tutela della riservatezza, appare molto sfumato, mentre ben concreto attuale e presente è il tema della tutela collettiva rispetto ad organizzazioni criminali tradizionali e oggi terroristiche le quali utilizzano costantemente e sistematicamente infrastrutture tecnologiche di comunicazione, talora più sofisticate ed avanzate rispetto agli strumenti pubblici di ricerca della prova informatica in dotazione alle forze di polizia, sicché una cosa è avvertire il problema della tutela della riservatezza (esigenza sicuramente presente nel richiamo diretto e costante all’art. 15 Cost. ma talora priva di riferimenti alla vigente normativa a tutela dei dati personali come il Codice per la protezione dei dati personali Decreto legislativo 30 giugno 2003, n. 196 che già offre una sovrabbondante piattaforma di garanzie istituzionali e individuali), ed un’altra criticare *in nuce* ogni strumento tecnologico oggi disponibile sul piano informatico, tanto più se utilizzato in concreto sotto (stretto) controllo giurisdizionale.

2009, 4, pp. 510-517; GUALTIERI P., *Prova informatica e diritto di difesa*, in *Diritto penale e processo*, 2008, 6S, pp. 70-74; ILLUMINATI G., *Accesso alle intercettazioni utilizzate in sede cautelare e diritto di co-*

pia, in *Giurisprudenza costituzionale*, 2008, 5, pp. 3761-3765; LA ROCCA E.N., *Misure cautelari e diritto all’ascolto delle intercettazioni*, in *La Giustizia penale*, 2008, 11/1, pp. 323-326.

5. LE INTERCETTAZIONI DIGITALI E LA PROVA DIGITALE NELLA PROSPETTIVA INTERNAZIONALE ED EUROPEA.

Va quindi precisato che il sistema informatico e telematico oggi può essere inteso anche come riferibile ad un singolo apparato telefonico¹⁰ e ciò in ragione del preciso disposto della Convenzione del Consiglio d'Europa sulla criminalità informatica (*Cybercrime*) di Budapest del 23 novembre 2001 cui l'Italia ha dato formale ratifica attraverso la legge 18 marzo 2008, n. 48 *“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”*.

La Convenzione all'art. 1 adotta una nozione estesa di “sistema informatico indicando appunto *qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati*. Secondo la Convenzione, inoltre, l'espressione “dati informatici” indica *qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato*, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione e per “trasmissione di dati” dovrà intendersi qualsiasi informazione computerizzata relativa ad una comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio.

Va sottolineato anche che la Convenzione prevede Articolo 20 la possibilità di *Raccolta in tempo reale di dati sul traffico*, che consente ad ogni parte aderente di adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie competenti autorità di: raccogliere o registrare attraverso l'utilizzo di strumenti tecnici nel suo territorio, obbligare un fornitore di servizi, nell'ambito delle sue capacità tecniche a: raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel suo territorio, o cooperare ed assistere le autorità competenti nella raccolta o registrazione in tempo reale di dati sul traffico associati a comunicazioni specifiche effettuate sul proprio territorio attraverso un sistema informatico.

¹⁰ In tal senso Sez. 2, Sentenza n. 5688 del 17/12/2004 che precisa come integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici o telematici di cui all'art. 615-*quater* cod. pen., la condotta di colui che si procura abusivamente il numero seriale di un *apparecchio telefonico cellulare* appartenente ad altro soggetto, poiché attraverso la corrispondente modifica del codice di un ulteriore apparecchio (cosiddetta clonazione) è possibile realizzare una illecita connessione alla rete di telefonia mobile, che costituisce un sistema telematico protetto, anche con riferimento alle banche concernenti i dati esteriori delle comunicazioni, gestite me-

diane tecnologie informatiche. Negli stessi termini Sez. 6, Sentenza n. 3067 del 04/10/1999 che ha ritenuto la possibilità di configurare accesso illecito a sistema informatico nel comportamento di indagati che, digitando da un apparecchio telefonico sito in una filiale italiana della società autorizzata all'esercizio della telefonia fissa un numero corrispondente a un'utenza extra urbana, e facendo seguire rapidamente un nuovo numero corrispondente a un'utenza estera, riuscivano a eludere il blocco del centralino nei confronti di tali telefonate internazionali, così abusivamente introducendosi nella linea telefonica e contestualmente procurandosi ingiusto profitto con danno per la società di esercizio telefonico).

È inoltre espressamente prevista la possibilità (Articolo 21) di *intercettazione di dati relativi al contenuto*, che rende legittime misure legislative e di altra natura che dovessero essere necessarie, in relazione ad una serie di gravi infrazioni che devono essere definite dal diritto nazionale, per consentire alle proprie competenti autorità di: raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte, e obbligare un fornitore di servizi, nell'ambito delle sue capacità tecniche a raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte, o infine cooperare ed assistere le autorità competenti nella raccolta o registrazione in tempo reale di dati relativi al contenuto di comunicazioni specifiche eseguite nel proprio territorio attraverso un sistema informatico.

Le predette misure sono intese riferibili (art. 14) ad un ambito di applicazione riferito sia ad indagini o procedimenti penali specifici, sia ad ogni reato *stricto sensu* "informatico" cioè commesso attraverso sistema o strumento informatico ai sensi degli art. 2/11 della Convenzione che, soprattutto *a tutti gli altri reati commessi attraverso un sistema informatico e all'insieme delle prove elettroniche di un reato*.

Di particolare interesse appare, ai fini delle problematiche delle intercettazioni "digitali" anche il successivo art. 15 che menziona specifiche condizioni e tutele per i (nuovi) strumenti investigativi, per cui ogni parte deve assicurarsi che l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste in questa sezione siano soggette alle condizioni e alle tutele previste dal proprio diritto interno, che deve assicurare un'adeguata tutela dei diritti umani e delle libertà, *in particolare dei diritti derivanti da obblighi assunti in base alla Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e delle libertà fondamentali, alla Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici, e agli altri strumenti internazionali applicabili in materia di diritti umani, e che deve considerare il principio di proporzionalità*.

In tal senso appare ben definito il concetto di "*intercettazione legale*" delle comunicazioni interpersonali, principio già contenuto nella Risoluzione del Consiglio del 17 gennaio 1995 sull'intercettazione legale delle telecomunicazioni (GU C 329 del 4.11.1996, pagg. 1-6). L'allegato contiene infatti *un elenco di condizioni per l'intercettazione legale da parte degli inquirenti*, delle quali gli Stati membri dovevano tenere conto nel definire ed attuare politiche e misure nazionali pertinenti. Infatti nella Convenzione (art. 21) quando sia il caso, avuto riguardo alla natura del potere o della procedura, queste condizioni e tutele devono includere, fra l'altro, *una supervisione giudiziaria* o di altra natura purché indipendente, *dei motivi che giustificano l'applicazione e la limitazione del campo di applicazione e della durata del potere o procedura*. Nella misura in cui ciò sia rispondente all'interesse pubblico e, in particolare, alla buona amministrazione della giustizia, ogni Parte deve infine considerare l'impatto dei poteri e delle procedure di intercettazione legale sui diritti, le responsabilità e gli interessi legittimi dei terzi.

Nell'Unione europea vige il principio generale della segretezza delle comunicazioni (e dei relativi dati circa il traffico). Le intercettazioni sono illecite salvo se *autorizzate dalla legge, nel caso siano necessarie in casi specifici per scopi limitati*. Questo principio è comunemente riportato all'articolo 8 della Convenzione europea dei diritti dell'uomo, cui fa riferimento l'articolo 6 del Trattato sull'Unione europea, e più in parti-

colare dalle direttive 95/46/CE e 97/66/CE. Quasi tutti gli Stati membri dell'Unione Europea sono dotati di un quadro normativo che consente a chi ha il compito di *garantire il rispetto della legge di ottenere l'ordine del giudice (o nel caso di due Stati membri, un mandato autorizzato personalmente da un ministro) per effettuare intercettazioni di comunicazioni sulle reti di telecomunicazioni*. Detta normativa interna, che deve essere comunque conforme al diritto comunitario nella misura in cui questo sia d'applicazione, prevede *misure di salvaguardia del diritto fondamentale dei cittadini alla tutela della vita privata*, quali ad esempio la *limitazione dell'utilizzo di intercettazioni alle indagini relative a reati gravi*, il requisito che le intercettazioni effettuate dagli inquirenti nei confronti di individui siano *strettamente necessarie e proporzionate*, o la garanzia che l'interessato sia informato dell'intercettazione, non appena ciò non interferisca con le indagini ¹¹.

È agevole sottolineare che il diritto italiano garantisce entrambe tali condizioni mediante la procedura definita dagli artt. 266 e 266 bis c.p.p. che, appunto prevedono un controllo giudiziario indipendente (nella specie da parte del giudice per le indagini preliminari) ben più rigido rispetto a quello definito in sede comunitaria, ed esteso, soprattutto alla verifica della funzionalità concreta dello strumento di ricerca della prova digitale, rispettando sia la limitatezza delle ipotesi di reato nelle quali tale strumento investigativo appare praticabile, sia — soprattutto — la delimitazione temporale della relativa utilizzazione ¹².

¹¹ *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni - Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica - eEurope 2002.*

¹² La questione della compatibilità dello strumento dell'intercettazione con l'art. 8 della Convenzione europea dei diritti umani era stata peraltro posto alla CEDU, che, occupandosi in particolare della normativa italiana ha sottolineato con decisione 11 giugno 2013 (ric. n. 11625/07) come la sorveglianza di una persona non possa essere limitata unicamente perché le utenze telefoniche di cui è titolare sono utilizzate anche da altre persone. Inoltre, quando un indiziato è in contatto con terze persone, è ben possibile che le autorità mettano sotto intercettazione anche le utenze telefoniche appartenenti ai terzi interessati, a condizione che questa ingerenza, conformemente alla legislazione nazionale, sia giustificata da una esigenza evidente. Al riguardo la Corte ha osservato come proprio l'articolo 267 del

c.p.p. prevede una garanzia sostanziale circa l'estensione temporale delle operazioni, con provvedimento argomentato del Giudice per le indagini preliminari soltanto se le intercettazioni sono «assolutamente indispensabili» per la prosecuzione dell'indagine. Con altra pronuncia del 10 aprile 2007 (ric. n. 46794/99), la CEDU aveva ritenuto non sussistenti le violazioni di cui agli articoli 8, 6 e 6 della Convenzione, mosse proprio in relazione alle intercettazioni ambientali ossia ad uno dei mezzi di ricerca della prova estremamente efficace nell'accertamento del reato, nonché in relazione al principio fondamentale dell'equo processo, recepito dalla Costituzione italiana all'art. 111. Importante è il rilievo in base al quale tal riguardo, ricorda la Corte ha ricordato che se la Convenzione europea obbliga i tribunali a motivare le loro decisioni, tale obbligo *non può però essere inteso come una richiesta di risposta dettagliata ad ogni argomento*. Vanno inoltre menzionate le decisioni 01/09/2015 (70462/13) 19/05/2015 (55546/09) 02/12/2014 (42733/07) 09/09/2014 (33955/07) tutte riferibili all'Italia e tutte confermate della coerenza della disciplina italiana delle intercettazioni sia telefoniche che telemati-

6. USO DEL TROJAN COME STRUMENTO INTERCETTATIVO: PROBLEMATICHE TECNICHE E GARANZIE EFFETTIVE.

Ma veniamo al punto. Con il termine Trojan ci si riferisce comunemente ai trojan ad accesso remoto (*detti anche RAT dall'inglese Remote Administration Tool*), composti generalmente da 2 file: il *file server*, che viene installato nella macchina vittima, ed un *file client*, usato dall'attaccante per *inviare istruzioni che il server esegue*. Un trojan può contenere qualsiasi tipo di istruzione e quindi può inserire sulla macchina ospite specifiche istruzioni eseguibili.

Ovviamente in un quadro di intercettazione legale l'inserimento di tali programmi, oltre che essere *espressamente autorizzato dal giudice* (in modo conforme ai requisiti richiesti in sede europea cui si è prima accennato) *corrisponde all'unica forma di captazione fonica* (e quindi sostanzialmente di intercettazione vocale) *praticabile rispetto all'uso di programmi di VOIP* sempre più diffusi e sempre più alla portata di tutti gli utenti di telefonia (Messenger, Facebook, Watsapp, Viber, Skype sono oggi disponibili gratuitamente su qualsiasi smartphone e ovviamente tali programmi consentono non solo l'invio simultaneo di messaggistica senza passare dal server del fornitore di accesso alla rete (telefonica mobile) ma connettendosi appunto in "cloud" (condivisione client-client) ai server privati esteri che gestiscono il relativo servizio ¹³.

In tal caso il programma può svolgere diverse funzioni, in larga parte semplificate e assimilabili ad un "tradizionale" sistema intercettativo (registrazione audio e video su una macchina dedicata con un sistema di duplicazione del segnale), e tale è di regola l'uso che si pratica con i sistemi VOIP.

Alcuni Trojan possono tuttavia eseguire comandi di attivazione di servizi esistenti sullo stesso apparato mobile "bersaglio" e quindi attivare automaticamente le funzioni di registrazione al verificarsi di certe condizioni (ad esempio in una certa cella o in presenza di contatti predeterminati) così semplificando le operazioni cognitive degli operatori sui contenuti, e tali funzioni possono estendersi a quelle di base, governate dal sistema operativo quali l'attivazione del microfono o della videocamera del terminale mobile (in pratica il telefonino o il computer possono trasformarsi se dotati di videocamera o di microfono in apparati intercettativi anche di alta qualità).

Tali opzioni intercettative, la cui intensità appare evidentemente allarmante, non possono però che avere (solo) nella argomentazione del provvedimento giurisdizionale autorizzatorio una regolamentazione concreta, che tenga conto della realtà investigata e, soprattutto, dei contesti specifici nei quali l'indagine si colloca, tanto più che ogni attività criminale tende ad utilizzare significati comunicativi non sempre decifrabili esplicitamente ed esposti ad interpretazione potenzialmente controvertibile.

che che "ambientali" con i principi della CEDU.

¹³ Cfr. TROGU M., *Le intercettazioni di comunicazioni a mezzo Skype*, in *Processo penale e Giustizia*, 2014, 3, pp. 8;

PARODI C., *VoIP, Skype e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?*, in *Diritto penale e processo*, 2008, 10, pp. 1309-1313.

Di qui, forse, la difficoltà del sistema normativo italiano, che da un lato sottopone a stretto controllo lo strumento mediante una penetrante verifica giudiziaria indipendente, e dall'altro di fronte alle nuove potenzialità tecniche di tale strumento, finisce per pretendere una regolamentazione quasi profetica degli ambienti frequentati dal soggetto intercettato nei suoi movimenti quotidiani, ben diversa peraltro dai limiti "oggettivi" che possono essere posti esclusivamente a livello di diretto precetto costituzionale (alla luce ad esempio del 4 emendamento della Costituzione degli Stati Uniti ¹⁴). Proprio tale funzione è stata problematicamente segnalata dalla dottrina ¹⁵ ed è stata oggetto delle prime valutazioni giurisprudenziali di legittimità, in un primo momento almeno orientate sul contenuto essenzialmente "documentale" delle acquisizioni digitali (Sez. U, Sentenza n. 6 del 23/02/2000) ¹⁶, per cui i dati di carattere informatico contenuti nel computer, in quanto rappresentativi, alla stregua della previsione normativa, di cose, rientrano tra le prove documentali (di recente Sez. 3, Sentenza n. 37419 del 05/07/2012). Più complessa appare la tematica della "registrazione" sistematica di contenuti digitali in particolari ambienti, tipicamente collegabile a sistemi informatici condivisi e quindi in uso a più soggetti, rispetto ai quali è certamente difficoltoso persino l'uso di uno strumento intercettativo non potendosi individuare con precisione ed esattezza effettiva gli utenti (ad esempio perché si tratta di risorse condivise o aperte ad uso comune, o magari perché vi è illecita sostituzione personale o accesso abusivo mediante credenziali di altro utente, o per la presenza di una rete wireless collettiva. In tal caso (Sez. 5, Sentenza n. 16556 del 14/10/2009) appare persino legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel "personal computer" in uso all'imputato e installato presso un ufficio pubblico, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e

¹⁴ Nella prospettiva statunitense tale disposizione costituzionale fa sì che non possa essere violato il diritto dei cittadini di godere della sicurezza personale, della loro casa, delle loro carte e dei loro beni, di fronte a perquisizioni e sequestri ingiustificati; e non si rilasceranno mandati di perquisizione se non su fondati motivi sostenuti da giuramento o da dichiarazione solenne e con descrizione precisa del luogo da perquisire e delle persone da arrestare o delle cose da sequestrare. È agevole osservare che in tale sistema giudiziario non ha una valenza probatoria diretta e che l'acquisizione probatoria si riferisce ad un "oggetto" o a un "documento" acquisito solo su mandato del giudice e solo con descrizione dettagliata.

¹⁵ TESTAGUZZA A., *I Sistemi di Controllo Remoto: fra normativa e prassi*, in *Diritto penale e processo*, 2014, 6, pp. 759-766.

¹⁶ Ai fini dell'acquisizione dei tabulati contenenti i dati esterni identificativi delle comunicazioni telefoniche conservati in archivi informatici dal gestore del servizio è sufficiente il decreto motivato dell'autorità giudiziaria, non essendo necessaria, per il diverso livello di intrusione nella sfera di riservatezza che ne deriva, l'osservanza delle disposizioni relative all'intercettazione di conversazioni o comunicazioni di cui agli articoli 266 e seguenti cod. proc. pen. (Nell'affermare tale principio la Corte ha altresì precisato che il controllo giurisdizionale sul provvedimento acquisitivo, che attiene ad un mezzo di ricerca della prova, si attua mediante la rilevabilità anche d'ufficio, in ogni stato e grado del procedimento, dell'eventuale inutilizzabilità, essendo l'art. 191 cod. proc. pen. applicabile anche alle c.d. prove "incostituzionali" perché assunte con modalità lesive dei diritti fondamentali).

contenuti nella memoria del “*personal computer*” o che in futuro sarebbero stati memorizzati ¹⁷.

È indubbio, tuttavia che dovrà tenersi conto, ai fini di una corretta risoluzione del problema delle c.d. “intercettazioni ubiquitarie”, cioè delle intercettazioni riferite ad apparato mobile e riferite all’indispensabile possesso dello strumento sulla persona del soggetto intercettato ed all’uso per le normali relazioni sociali di questi della impossibilità di distinguere nettamente il profilo della intercettazione dei contenuti (vocali o testuali, ad esempio estratti dai servizi di messaggistica) laddove questi siano legittimamente oggetto di un procedimento acquisitivo conforme con il requisito comunitario di “legalità” (ovvero in sostanza soggetto a controllo giurisdizionale) e per le quali l’uso di un programma informatico (scaricato inconsapevolmente dal soggetto intercettato sul suo sistema) finisce solo per essere uno strumento irrilevante e di mera introduzione tecnica nel sistema informatico oggetto di captazione previamente autorizzata dal giudice ed in parte equiparabile anche ad una intercettazione ambientale (in quanto appunto conforme ai requisiti di cui all’art. 266 comma 2 c.p.p.) seguendo un concetto di “domicilio” non più, forse, collegabile ad un “luogo” (appunto oggetto di perquisizione e sequestro anche sul piano informatico ora con l’introduzione dell’art. 254-bis c.p.p. introdotto appunto con la legge 18 marzo 2008, n. 48) ma ben ricollegabile (dinamicamente) alle relazioni sociali “contattate” da un utente ben individuato con l’uso di un apparato software ed hardware in suo possesso. Si è già detto che, con riguardo alla criminalità organizzata ed al terrorismo le indagini possono ben derogare ai limiti posti in relazione alle esigenze di tutela del domicilio. Una compressione eccessiva del ricorso alle opportunità investigative della prova digitale rischia di produrre, per altro verso, un sostanziale vuoto normativo che finirebbe proprio per ostacolare, se non proprio precludere l’acquisizione probatoria in relazione, appunto, ai reati sintomatici di una più vasta ed articolata organizzazione criminosa.

È del pari evidente che, a causa delle caratteristiche intrinseche dello strumento del sequestro (probatorio) per l’acquisizione di contenuti digitali vi sia il rischio di integrale compromissione dell’indagine nel suo insieme prospettico e funzionale tanto più con riguardo a particolari categorie di reati gravi caratterizzati tutti da un contesto organizzativo e relazionale consistente, che può essere facilmente eluso proprio con ricorso alle tecnologie informatiche (ricorso a messaggistica collegata a determinate applicazioni condivise, o a codici figurativi allegati a testi, convenzionalmente utilizzati come simbolo di determinate reazioni o condotte, tanto più in un contesto tipico dei c.d. “reati spia” e cioè logicamente e ontologicamente ricollegabili ad una organizzazione criminosa in corso di accertamento e di identificazione completa).

¹⁷ Nel caso di specie, l’attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull’“hard disk” del computer in uso all’imputato, aveva avuto ad oggetto non un “flusso di comunicazioni”, richiedente un dialogo con altri soggetti, ma “una relazione operativa tra microprocessore e video del sistema elettro-

nico”, ossia “un *flusso unidirezionale di dati*” confinati all’interno dei circuiti del computer; la S.C. ha perciò ritenuto corretta la qualificazione dell’attività di captazione in questione quale *prova atipica, sottoposta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen.*

In realtà la motivazione della Corte nelle sue posizioni più recenti lascia spazio a due distinti profili problematici.

Il primo è quello della compatibilità in sé del mezzo intercettativo “ubiquitario” con l’art. 15 Cost., il secondo consiste nel limite attraverso il quale *il controllo sulla motivazione del provvedimento autorizzatorio* (caratteristica anch’essa posta a livello costituzionale) può incontrare dal punto di vista prima logico e poi tecnologico in quanto una volta posto in essere il procedimento acquisitivo non appare agevole distinguere in concreto (e quindi tanto più prevedere in astratto) i movimenti del soggetto nello spazio e soprattutto i comportamenti relazionali che si estrinsecano proprio nell’uso di tecnologie comunicative sempre più sofisticate proprio al fine di eludere le intercettazioni legittimamente disposte e giustificate da un grave quadro indiziario. Il profilo appare significativo e l’eventuale limitazione di possibilità investigative con riguardo a reati prodromici di tipo associativo (si pensi solo all’estorsione o alla minaccia rispetto al reato di associazione a delinquere di cui all’art. 416-bis o a richieste di voto di scambio o di gestione di appalti pubblici nel medesimo contesto) potrebbe definirsi nettamente.

La questione — di un certo rilievo costituzionale — non è nuova per chi ha seguito tale problematica in un contesto internazionale, alla luce degli interrogativi già postisi in Germania¹⁸, e si tratta quindi di tracciare ora un punto di equilibrio tra esigenze investigative e di sicurezza collettiva che appaiono oggi essenziali e entro certi limiti addirittura prevalenti, dato il contesto organizzato e tecnologicamente connotato di criminalità organizzata comune e terrorismo internazionale, ed esigenze di tutela effettiva dell’individuo che non possono però essere affrontate con richiami generici o con soluzioni interpretative inconsapevoli della realtà delle attuali tecnologie comunicative informatiche.

GIUSEPPE CORASANITI

¹⁸ Si tratta della sentenza della Corte costituzionale tedesca del 27 febbraio 2008 (Brv 370/07 e Brv 595/07. Su cui cfr. FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona*, in *Rivista trimestrale di diritto penale dell’economia*, 2009, 3, pp.

695-716; ARGIRÒ F., *L’ammissibilità delle intercettazioni telematiche (on-line Durchsuchungen) al vaglio del Bundesgerichtshof: il caso dei c.d. Bundestrojaner*, in *Archivio penale*, 2008, 1, pp. 263-276. Il tema è particolarmente approfondito da ATERNO S. in AA.VV., *Commento all’art. 8 della legge 18 marzo 2008 n. 48 in Cybercrime, responsabilità degli enti e prova digitale* (a cura di G. Corasaniti e G. Corrias Lucente), Padova 2009 p. 215.