Corte di Cassazione, Sezioni Unite Penali, informazione provvisoria n. 15 del 28 aprile 2016

Con la sentenza n. 27100 del 26 maggio 2015 era stata rimessa alle Sezioni Unite la seguente questione di diritto in tema di intercettazioni tramite virus informatico: "*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.).*" All'udienza del 28 aprile 2016, la Cassazione, a sezioni unite, ha fornito la seguente soluzione: "*Affermativa, 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.*"

di Giuseppe Corasaniti

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

Giuseppe CORASANITI, è Sostituto Procuratore Generale della Procura generale della Repubblica presso la Corte Suprema di Cassazione. Studioso tra i più esperti di problemi giuridici della comunicazione e dell'informatica e di Diritto informatico. È autore di numerosi studi in tema di libertà e diritti fondamentali e comunicazione interattiva. È docente universitario a contratto di informatica giuridica presso l'Università degli Studi di Roma "La Sapienza".

La questione della legittimità delle intercettazioni di contenuti sonori o video operata a distanza con attivazione di programma applicativo inoculato nel dispositivo telefonico mobile è stata di recente trattata dalle S.U. della cassazione, e il tema – tanto più nell'attuale contesto - si presenta quanto mai controverso e delicato[1].

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 considerare 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 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.***"[2]

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"***.

1 La questione è stata infatti esaminata nell'ordinanza della 6 sez. penale 10 marzo – 6 aprile 2016, n. 13884, che ha posto 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 tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, cod. proc. Pen., se possa comunque prescindersi da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata.

2 Secondo la Corte, infatti, in giurisprudenza, si ammetterebbe la variazione dei luoghi in cui deve svolgersi la captazione solo se rientrante 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).

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.*"[3] 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 terrorismo[4] 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 "*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 (*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").

È ben noto il rischio di vanificare del tutto – mediante una interpretazione di carattere strettamente formale – 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.
Va quindi precisato che il sistema informatico e telematico **oggi può essere inteso anche come riferibile ad un singolo apparato telefonico** e ciò in ragione del preciso disposto della Convenzione del Consiglio d'Europa sulla criminalità informatica (*Cybercrime*) di Budapest del 23 novembre 2001cui l'iItalia 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*

3 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, perchè 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, sicchè, quando si tratta di 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).

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

dell'ordinamento interno". 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).

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 giustifichino 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.* 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.[5]

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, Watzapp,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.[6] 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 quasi tutti i sistemi VOIP. 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.

Il problema assai delicato, che viene poi a definirsi, è quello di garanzia dell'integrità del sistema intercettato e dei dati in esso contenuti subito dopo l'immissione del Trojan, apparendo evidente che il contesto internazionale richiede specifiche cautele (ben definite nella Convenzione sul Cybercrime del 2001) di non alterazione di dati e informazioni e che, tanto più in un contesto giurisdizionalmente controllato quale quello italiano, occorre coordinare il profilo acquisitivo sotto l'aspetto delle garanzie tecniche e della assoluta ricostruibilità delle operazioni informatiche svolte dopo l'immissione del programma, sicché appare indispensabile che tali operazioni siano documentate e attestate analiticamente dalle forze di polizia specializzate appositamente delegate. 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 [7]).

5 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 CPP 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 confermative della coerenza della disciplina italiana delle intercettazioni sia telefoniche che telematiche che "ambientali" con i principi della CEDU.

6 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.

7 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. E' agevole osservare che in tale sistema giudiziario non ha una valenza probatoria diretta e che l'acquisizione probatoria si rifersice ad un "ogegtto" o a un "documento" acquisito solo su mandato del giudice e solo con descrizione dettagliata.

Proprio tale funzione è stata problematicamente segnalata dalla dottrina[8] 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)[9], 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).

È indubbio, tuttavia, che dovrà tenersi conto, ai fini di una corretta risoluzione del problema, 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 e dell'**impossibilità di distinguere nettamente il profilo dell'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.

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 Germania[10], 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 – tenendo conto anche del contesto articolato, transnazionale 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. ©

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

9 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).

10 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 Bundesgerichthof: 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 .