

Mezzi di ricerca della prova informatica e garanzie difensive: dagli accertamenti investigativi al virus di Stato – 15 luglio 2015

Le indagini atipiche – Perquisizioni *on line* e
captatore informatico nel diritto vivente

Marco Torre

Definizione

I "captatori informatici" sono software che, una volta installati (furtivamente) all'interno di un determinato sistema informatico obiettivo, consentono ad un centro remoto di comando di prenderne il controllo, sia in termini di download che in termini di upload di dati e informazioni di natura digitale. Il software è costituito da due moduli principali, un programma server ed un programma client: il server è il programma di piccole dimensioni che infetta il dispositivo "bersaglio"; il client, invece, è l'applicativo che il "pirata" usa per controllare il dispositivo infetto.

Modalità di intrusione

Da remoto

In questo caso il collegamento tra client e server viene realizzato a distanza, attraverso l'invio, tramite la rete internet, di un c.d. virus trojan, cioè un programma ambiguo, dalla doppia faccia, costituito da una componente nota all'utente, il quale installa il programma proprio per ottenere le funzionalità a lui familiari, e una componente non nota (il cavallo di Troia, appunto), rappresentata da quella parte del programma che cela un codice segreto in grado di creare un collegamento occulto tra il dispositivo su cui è installato il server ed il computer remoto di controllo. Tale collegamento, che consente di fatto all'utente del computer remoto di avere il pieno controllo del sistema informatico "bersaglio", viene creato inconsapevolmente dall'utente di quest'ultimo attraverso l'installazione del programma nella sua componente nota e palese.

Da vicino

In questo caso il collegamento tra client e server viene realizzato intervenendo fisicamente a livello hardware sul dispositivo da controllare: l'intervento tecnico, in questo caso, consiste nell'inserimento, da parte del controllore, di una backdoor all'interno del dispositivo "bersaglio" in maniera del tutto simile a quanto avviene per l'installazione di una microspia finalizzata ad una intercettazione ambientale.

Aspetto tecnico-operativo

On line search	On line surveillance
I programmi spia consentono di far copia, totale o parziale, delle unità di memoria del sistema informatico "attenzionato". In particolare, i software sono tecnicamente in grado di entrare in maniera occulta all'interno del dispositivo "bersaglio" al fine di estrapolarvi dati e informazioni che, una volta "copiati", vengono trasmessi, in tempo reale o ad intervalli prestabiliti, agli organi di investigazione, ad un indirizzo internet prestabilito, tramite la rete Internet, in modalità nascosta e protetta . Ai nostri fini, più che di "captatore", bisognerebbe più specificatamente parlare di "copiatore informatico" .	I programmi spia consentono di monitorare il flusso di dati che coinvolgono un determinato sistema informatico o telematico. In particolare, se il dispositivo è collegato ad altri dispositivi attraverso una rete domestica o aziendale, o se, comunque, il computer è connesso ad internet, attraverso i software è possibile monitorare tutti i dati relativi alle sue comunicazioni con la rete medesima (ora e durata della connessione, invio e ricezione di e-mail, chat, siti internet visitati, files scaricati, ecc.). Con riferimento a tale tipologia di programma, sarebbe più corretto parlare di "appostamento informatico" .

Aspetto tecnico-giuridico

La questione della legittimità dei nuovi *investigative tools* e dei loro limiti viene solitamente affrontata in base ad uno schema logico-argomentativo - imposto dal principio di “legalità temperata” delle prova vigente nel nostro sistema processuale– che consta di tre propedeutici livelli:

1° LIVELLO

Verifica della effettiva “atipicità” dello strumento investigativo: individuare un modello tipico in cui ricondurre le perquisizioni on line, infatti, significherebbe risolvere ex lege quella valutazione di legittimità dello strumento investigativo che, altrimenti, è rimessa totalmente all’interprete

2° LIVELLO

Valutazione della possibilità di sfruttare, o meno, l’art. 189 c.p.p. per legittimare il mezzo atipico di ricerca della prova: l’applicabilità della norma dedicata dal codice di rito alla prova atipica dipende, innanzitutto, dal rispetto dei requisiti sostanziali e processuali che tale disposizione prevede.

3° LIVELLO

Verifica della esistenza, o meno, di eventuali limiti di natura costituzionale. Come noto, infatti, il primo presupposto di validità di una prova atipica è la sua legittimità costituzionale. Occorre, quindi, individuare il “tipo” di bene giuridico attinto dal mezzo investigativo qualificato come atipico, onde verificarne “rango” ed “intensità” di compressione.

1° LIVELLO

Verifica della effettiva atipicità dello strumento investigativo

Nella ricerca di un modello tipico in cui ricondurre le perquisizioni *on line* si deve adottare un canone ermeneutico di interpretazione tassativa. Infatti, per diretto mandato costituzionale in queste ipotesi la norma processuale penale è volta a dare attuazione alla riserva di legge, ovvero a stabilire i “casi e modi” attraverso cui i pubblici poteri possono attingere diritti altrimenti definiti inviolabili: casi e modi insuscettibili, pertanto, di interpretazioni analogiche o estensive

Andando alla ricerca della tipicità, le perquisizioni *on line* potrebbero essere accostate e confrontate con:

- le ispezioni (artt. 244 e ss. c.p.p.)
- le perquisizioni (artt. 247 e ss. c.p.p.)
- le intercettazioni (artt. 266 e ss. c.p.p.)

Ispezioni	Perquisizioni on line
Ispezione (art. 244): osservare e descrivere persone, luoghi e cose allo scopo di accertare le tracce e gli altri effetti materiali del reato L'ispezione è atto conoscibile dall'indagato: il pubblico ministero, se vuole procedere ad ispezione, deve preavvertire la persona sottoposta alle indagini (art. 364, co. 1); il difensore ha il diritto di assistere (art. 364, co. 4); anche nei casi di maggiore urgenza, è sempre fatta salva la facoltà del difensore di intervenire (art. 364, co. 5). Il verbale è depositato nella segreteria del pubblico ministero ed il difensore ha la facoltà di esaminarlo e di estrarne copia	Le perquisizioni on line risultano totalmente estranee alla funzione denotativo-descrittiva, tipicamente statica, delle ispezioni, essendo atte ad una subdola raccolta, anche prolungata nel tempo, di dati e informazioni di pertinenza dell'indagato, a sua insaputa Sono atti ignoti all'indagato durante il loro svolgimento, non conoscibili e non depositati, in relazione ai quali l'indagato non può esercitare diritti di difesa: le garanzie legali previste per le ispezioni frusterebbero radicalmente gli scopi di qualsiasi perquisizione on line.

Perquisizioni tradizionali	Perquisizioni on line
Le perquisizioni (art. 247) possono essere personali e locali e sono strutturalmente orientate alla ricerca del corpo del reato e/o delle cose pertinenti al reato che, in caso di reperimento, vengono senz'altro sequestrate Sono sì atti a sorpresa, nel senso che non deve essere dato previo avviso del loro compimento all'indagato, ma sono atti conoscibili dall'indagato, il quale ha diritto ad una serie di adempimenti in chiara funzione garantistica: notifica del decreto motivato (art. 250); invito a nominare un difensore di fiducia ovvero, in mancanza, designazione di un difensore d'ufficio, con conseguente diritto di farsi assistere dal difensore (art. 365); deposito del verbale e notifica dell'avviso di deposito (art. 366)	Si svolgono per lo più in quel luogo virtuale che è il web, possono prescindere dalla ricerca del corpo del reato e/o delle cose pertinenti al reato e non sfociano necessariamente in un sequestro Sono atti ignoti all'indagato durante il loro svolgimento, non conoscibili e non depositati, in relazione ai quali l'indagato non può esercitare diritti di difesa: le garanzie difensive previste per le perquisizioni tradizionali frusterebbero radicalmente gli scopi di qualsiasi perquisizione on line

Intercettazioni

Il common core delle intercettazioni (art. 266) è dato dalla captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscono con l'intenzione di escludere altri e con modalità tecniche oggettivamente idonee allo scopo (definizione che si deve ritenere applicabile anche alle intercettazioni di comunicazioni informatiche o telematiche intercorrenti tra utenti del web). Lo scopo è quello di assicurare al processo dichiarazioni o comunicazioni

Cass., sez. un., 24 settembre 2003, Torcasio, in Guida dir., 2003, n. 42, p. 49

Perquisizioni on line

Le perquisizioni on line sono concepite per ottenere un elevato numero di informazioni utili senza alcuna necessità di percepire comunicazioni in atto tra utenti, bensì semplicemente attraverso la sistematica o periodica raccolta di dati presso il sistema informatico utilizzato dall'indagato (on line search) o attraverso la registrazione dei suoi movimenti sul web (on line surveillance). Sotto il profilo tecnico, muoversi nella rete comporta necessariamente lo scambio di dati tra più sistemi informatici o telematici, tuttavia tali comunicazioni non intercorrono tra utenti persone fisiche.

Cass., sez. V, 14 ottobre 2009, Virruso ed altri, in CED Cass., n. 246954

Cass., sez. V, 14 ottobre 2009, Virruso

È 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 contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati. (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 elettronico", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen.)

Critica

Tecnicamente, il p.m. autorizzava tale attività, in data 22.04.2004, tramite "decreto di acquisizione di atti", ai sensi dell'art. 234 c.p.p. In realtà, il decreto disponeva l'acquisizione non solo dei files già esistenti (preesistenti al provvedimento), ma anche di tutti quei dati che sarebbero stati inseriti in futuro nella memoria del personal computer in uso al soggetto indagato (formati dopo il provvedimento), realizzando in tal modo un vero e proprio monitoraggio occulto e continuativo del contenuto della memoria di massa del computer “infetto” (protrattosi per oltre otto mesi), attività che esula evidentemente dalla *ratio* dell'art. 234.

2° LIVELLO

Verifica dell'applicabilità dell'art.189 c.p.p.

- 1) Idoneità ad assicurare l'accertamento dei fatti: la prova atipica deve essere in concreto capace di fornire elementi attendibili e di permettere una valutazione sulla credibilità della fonte di prova;
- 2) Rispetto della libertà morale della persona-fonte di prova: la prova atipica deve lasciare integra la facoltà di determinarsi liberamente rispetto agli stimoli (si vuole garantire l'esclusione di influenze *ab extra* sul processo volitivo della persona)
- 3) Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.

Sul requisito procedurale dell'art. 189

Tesi minoritaria	Tesi maggioritaria
I mezzi di ricerca della prova sono posti in essere prevalentemente nel corso delle indagini preliminari, senza previo contraddittorio con la difesa. Pertanto, si afferma, sarebbe impossibile dare attuazione all'art. 189 c.p.p. nella parte in cui impone che il giudice senta le parti sulle modalità di assunzione della prova prima di decidere con ordinanza sulla richiesta di ammissione.	Interpretazione adeguatrice dell'art. 189: qualora l'atipicità riguardi mezzi di ricerca e non mezzi di prova, anziché configurare un contraddittorio anticipato sulla ammissione nel corso delle indagini, si potrà e dovrà svolgere un contraddittorio successivo in dibattimento sulla utilizzabilità degli elementi acquisiti.

Sul requisito procedurale dell'art. 189

Tesi minoritaria	Tesi maggioritaria
La tesi che predica l'applicazione dell'art. 189 c.p.p. alla fase delle indagini, pur se animata dal condivisibile intento di recuperare delle forme di tutela per la persona sottoposta alle indagini, si rivela [...] totalmente inadeguata allo scopo, ed anzi soggetta al rischio di ipocrite strumentalizzazioni». Ciò a causa dello svilimento della portata garantistica propria dell'art. 189 c.p.p., provocato da un recupero ex post del contraddittorio tutt'altro che effettivo e dall'assenza di qualsiasi controllo giurisdizionale in itinere. Cfr. S. Marcolini, <i>Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta</i>, in <i>Cass. pen.</i>, 2, 2015, pp. 760 e ss.	Noi riteniamo che la soluzione del problema passi attraverso i principi generali del sistema: l'art. 189, non a caso, è posto all'interno del Titolo I del Libro III sulle prove, e cioè tra quelle "disposizioni generali" che costituiscono un catalogo di principi guida in materia probatoria, come tali applicabili "all'intero arco del procedimento, anche in via analogica, fuorché nei casi in cui norme speciali dettate per le diverse fasi, o peculiari previsioni legge, non le derogano". Cfr. M. Nobili, <i>sub art. 189 c.p.p.</i>, in AA.VV., <i>Commento al nuovo codice di procedura penale</i>, coordinato da M. Chiavario, tomo II, Torino, 1990.

Cass, sez. un., 28 marzo 2006, n. 26795 (Prisco)

«Il contraddittorio previsto dall'art. 189 non riguarda la ricerca della prova, ma la sua assunzione e interviene dunque, come risulta chiaramente dalla disposizione, quando il giudice è chiamato a decidere sull'ammissione della prova»

In tema di videoriprese, cfr. Cass., sez. un., 28 marzo 2006, Prisco, in *Dir. pen. proc.*, 2006, p. 1347.

3 ° LIVELLO

Verifica di eventuali limiti di natura costituzionale

L'aver risolto negativamente il quesito sulla tipicità e positivamente quello sull'applicabilità dell'art. 189 c.p.p. non significa ancora aver raggiunto un risultato appagante: come noto, infatti, il primo presupposto di validità di una prova atipica è la sua legittimità costituzionale. Occorre, quindi, individuare il "tipo" di bene giuridico attinto dal mezzo investigativo qualificato come atipico, onde verificarne "rango" ed "intensità" di compressione. Dal posto che il bene occupa all'interno di tale ideale scala gerarchica e dall'intensità della sua potenziale lesione dipende la legittimità dello strumento atipico e la conseguente utilizzabilità, o meno, dei risultati con esso ottenuti

Rango dell'interesse protetto

Punto di partenza della nostra riflessione è che, a livello sistematico, sono ipotizzabili almeno tre livelli decrescenti di garanzie del privato di fronte a possibili atti di indagine compiuti nei suoi confronti da parte delle autorità inquirenti pubbliche: ad ogni livello corrisponde un diverso *standard* di tutela e la graduazione dipende dal “rango” dell'interesse in gioco:

Libertà personale, domicilio e corrispondenza, ex artt. 13, 14 e 15 Cost.: riserva di legge e riserva di giurisdizione.

Riservatezza, ex art. 2 Cost., nuovi diritti o diritti di seconda generazione (situazioni giuridiche soggettive la cui crescente importanza rappresenta il segno tangibile dell'evoluzione della coscienza sociale e la cui copertura costituzionale viene individuata nell'ambito dell'art. 3 Cost.): solo riserva di giurisdizione, almeno secondo l' “approccio funzionale” della giurisprudenza di legittimità (Cass., sez. un., 28 marzo 2006, n. 26795, Prisco)

The *right to be left alone* (es., aspettativa di riservatezza in un luogo pubblico e altre situazioni nelle quali non esiste alcuna aspettativa giuridicamente azionabile da parte del privato a fronte del potere-dovere dell'autorità di indagare): nessuna riserva.

Diritti fondamentali coperti da riserva di legge e di giurisdizione

A fronte di “diritti fondamentali” coperti da riserva di legge rinforzata dalla necessità, da parte del legislatore, di prevedere i “casi” e i “modi” di una loro possibile limitazione, il fine accertativo del processo penale deve viaggiare sui precisi binari tracciati dal legislatore e la rotta deve essere controllata dall’Autorità giudiziaria. In base alla teoria della c.d. “prova incostituzionale”, ne consegue l’inammissibilità del mezzo atipico di ricerca della prova che mette a repentaglio tali diritti e, comunque, l’inutilizzabilità dei risultati con esso ottenuti.

Cfr. V. Grevi, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. Cost.*, 1973, p. 341.

Sulla prova incostituzionale

Oggi, l'autentica difficoltà dell'interprete non consiste nello stabilire se una prova incostituzionale è utilizzabile, bensì nel valutare se una prova è incostituzionale.

Per stabilire ciò, l'interprete deve effettuare tre valutazioni caratterizzate da una forte componente di discrezionalità:

- 1) anzitutto, si deve individuare l'interesse protetto dalla norma violata;
- 2) in secondo luogo, si deve stabilire il rango di tale interesse;
- 3) infine, deve essere ponderato il grado di lesione che la tipologia atipica di acquisizione comporta, anche nel bilanciamento con gli altri interessi rilevanti nella fattispecie.

Con le seguenti precisazioni:

- soltanto in presenza di una significativa compromissione del nucleo centrale dell'istanza costituzionale la prova atipica è inutilizzabile;
- viceversa, qualora venga in gioco un diritto fondamentale, ma il grado della lesione appaia non tanto rilevante da intaccarne l'essenza, la prova è utilizzabile purché sia introdotta con provvedimento motivato del pubblico ministero;
- infine, ove non sia inciso in alcun modo un interesse di tale rango, la prova atipica è utilizzabile secondo le regole generali (art. 189 c.p.p.), anche qualora l'acquisizione sia effettuata nel corso delle indagini preliminari su semplice iniziativa della polizia giudiziaria.

Il modello di tutela dipende, dunque, dal bene giuridico che si ritiene inciso dall'acquisizione e la ricognizione dello stesso richiede un'attività valutativa ad altissimo tasso di discrezionalità in assenza di riferimenti di diritto positivo

Sulla prova incostituzionale

Con tale sintagma dottrina e giurisprudenza sono solite indicare quegli elementi di prova che vengono acquisiti con modalità non disciplinate dal codice di rito e lesive dei diritti fondamentali dell'individuo costituzionalmente tutelati.

Su questo tema, in dottrina, si sono formati orientamenti differenti:

- teoria che nega la stessa esistenza della categoria concettuale della “prova incostituzionale”;
- teoria dell'interpretazione estensiva dell'art. 191, comma 1, c.p.p.;
- teoria dell'interpretazione adeguatrice dell'art. 189 c.p.p. (tesi dei divieti impliciti).

Teoria “negazionista”

- Vi è chi ritiene che l'art. 189 non impedisca l'ingresso delle prove atipiche lesive dei diritti fondamentali. L'assenza di una norma di legge ordinaria che vieti acquisizioni del genere, infatti, impedirebbe di sanzionare la prova atipica incostituzionale; conseguentemente, è stata ritenuta l'utilizzabilità processuale dell'elemento acquisito
- All'interno di tale posizione esegetica spicca quell'orientamento che, facendo leva sui rilievi appena svolti, ritiene l'incostituzionalità dell'art. 189 c.p.p. nella parte in cui non prevede i casi e i modi in cui consentire l'ingresso di prove atipiche lesive di diritti fondamentali (questo significa, evidentemente, che per non consentire l'ingresso e l'utilizzo di prove incostituzionali, bisognerebbe sollevare questione di costituzionalità; fintantoché ciò non accade, la prova è utilizzabile)

Teoria dell'interpretazione estensiva dell'art. 191, comma 1, c.p.p.

Un differente indirizzo prospetta un'interpretazione estensiva dell'espressione “divieti stabiliti dalla legge” prevista dall'art. 191, comma 1, in tema di inutilizzabilità. In base a questa tesi, nel concetto di “legge” inteso, appunto, estensivamente, rientra anche la Carta fondamentale. La conseguenza è che gli atti acquisitivi non espressamente previsti dalla legge, ma lesivi di diritti fondamentali, sono vietati. La violazione di tali “divieti probatori costituzionali” rinviene la sua sanzione e la sua disciplina nell'art. 191

Teoria dell'interpretazione adeguatrice dell'art. 189 c.p.p. (tesi dei divieti impliciti)

Poiché l'art. 189 c.p.p., nell'ammettere le prove atipiche, non determina i casi e i modi con i quali prove di tal genere possono ledere i diritti fondamentali, una lettura conforme a Costituzione impone di ritenere che proprio in ragione di tale silenzio l'art. 189 precluda l'ingresso processuale di simili esperimenti conoscitivi. La conseguenza è che l'elemento probatorio acquisito in violazione di questo "divieto implicito" è inutilizzabile ex art. 191, comma 1

Diritti coperti dalla sola riserva di giurisdizione

Nella fase delle indagini preliminari, lo svolgimento del mezzo atipico di ricerca della prova lesivo di questa tipologia di diritti rientra tra le facoltà previste dagli artt. 55, 347 e 370 c.p.p., con la necessità, tuttavia, di un previo e congruamente motivato provvedimento dell'autorità giudiziaria (quindi, anche del p.m.); in dibattimento, i suoi risultati possono essere utilizzati nel rispetto dei requisiti sostanziali di cui all'art. 189 c.p.p., previa ammissione da parte del giudice, il quale dovrà sentire le parti in contraddittorio sulle modalità di assunzione.

In questi casi, in assenza di stretti vincoli costituzionali ed in mancanza di precise regole codicistiche, il bilanciamento tra opposti interessi –pur doveroso- spetta all'autorità giurisdizionale.

L'atto motivato dell'autorità giudiziaria rappresenta quel “livello minimo di garanzie” necessario ma anche sufficiente per garantire un giusto equilibrio tra la tutela dei diritti dei soggetti coinvolti nel procedimento penale e l'esigenza di accertamento del fatto di reato e di punizione dei colpevoli.

Sul “livello minimo di garanzie”: Corte costituzionale, sentenza n. 81 del 1993.

“Ferma restando la libertà del legislatore di stabilire norme di attuazione dei principi costituzionali, il livello minimo di garanzie [...] –che esige con norma precettiva tanto il rispetto di requisiti soggettivi di validità in ordine agli interventi nella sfera privata relativa alla libertà di comunicazione (atto dell’autorità giudiziaria, sia questa il pubblico ministero, il giudice per le indagini preliminari o il giudice del dibattimento), quanto il rispetto di requisiti oggettivi (sussistenza e adeguatezza della motivazione in relazione ai fini probatori concretamente perseguiti)- pone un parametro di validità che spetta al giudice *a quo* applicare direttamente al caso di specie, al fine di valutare se l’acquisizione del tabulato, contenente l’indicazione dei riferimenti soggettivi, temporali e spaziali delle comunicazioni telefoniche intercorse, possa essere considerata legittima e, quindi, ammissibile”.

Questo è il ragionamento seguito dalla Corte Costituzionale con riferimento alla acquisizione dei tabulati telefonici prima della entrata in vigore del codice della privacy che ne ha compiutamente disciplinato l’utilizzazione per fini investigativi.

... e Corte costituzionale, sentenza n. 281 del 1998.

La Corte costituzionale, pur auspicando “che il legislatore provveda a disciplinare in modo organico l’acquisizione e l’utilizzazione della documentazione relativa al traffico telefonico, in funzione della specificità di questo particolare mezzo di ricerca della prova, che non trova compiuto sviluppo normativo nella disciplina generale prevista dal codice in tema di dovere di esibizione di atti e documenti e di sequestro”, precisa che nel caso *de quo* “il livello minimo di garanzie [...] risulta allo stato rispettato per l’aspetto specificatamente dedotto della autorizzazione del pubblico ministero all’acquisizione dei tabulati”.

Tale “livello minimo di garanzie”, chiarisce la Corte, consta di due fondamentali requisiti: un requisito soggettivo, consistente nella necessità che l’attività atipica sia stata preventivamente autorizzata attraverso un atto del pubblico ministero o del giudice; un requisito oggettivo, che si traduce nell’obbligo che tale atto autorizzativo abbia un’adeguata motivazione in relazione ai fini probatori concretamente perseguiti attraverso lo strumento atipico di indagine.

Nessuna riserva

Per lo svolgimento di attività di indagine atipica non lesiva di aspettative meritevoli di tutela non è necessario alcun provvedimento giurisdizionale. I risultati ottenuti, evidentemente, verranno filtrati ex art. 189 c.p.p. D'altronde, l'opportunità di legittimare indagini atipiche si legge a chiare lettere nella Relazione che accompagna il codice di rito. La ratio, ovviamente, è di evitare un eccessivo "ingessamento" dell'attività della polizia giudiziaria e del pubblico ministero, a discapito della efficienza delle rispettive indagini.

Il bene giuridico in gioco

Il mezzo di indagine oggetto di riflessione consente la raccolta di una mole impressionante ed indiscriminata di dati personali all'insaputa del soggetto attinto (e di quelli con cui entra in contatto), per un tempo indeterminato. Nel momento in cui il c.d. virus informatico consente di monitorare tutto ciò che il soggetto attenzionato scrive, anche se poi decide di cancellare ciò che ha appena scritto, si pone addirittura un problema di "inviolabilità della psiche". D'altronde, utilizzare un computer, oggi, è quanto di più quotidiano e di intimo si possa fare. L'uso della tecnologia informatica, infatti, ha assunto un significato nuovo e diverso per la personalità individuale e lo sviluppo della persona, non prevedibile fino a pochi decenni fa. I sistemi informatici sono ormai onnipresenti e il loro uso è un elemento centrale per la vita di ogni cittadino. I dati che gli utenti creano o conservano rappresentano informazioni aventi ad oggetto il comportamento degli utenti stessi, le loro situazioni personali e le attività svolte. In sostanza, da tali dati è possibile ricavare elementi sulla personalità degli individui, attraverso una vera e propria "profilazione".

Riservatezza

Sul versante delle garanzie coinvolte, le perquisizioni on line incidono – quantomeno – sulla bene giuridico della riservatezza, sub specie “riservatezza informatica”. “Tale diritto nasce come espansione del domicilio per acquistare autonomia in un ambito, quello digitale, in cui non ci sono confini, non ci sono luoghi fisici che possano riflettere il carattere privato o riservato delle attività che ivi si svolgano o di ciò che vi sia custodito” (Così, F. Iovene, *Le c.d. perquisizioni on line tra nuovi diritti fondamentali ed esigenze di accertamento penale*, www.penalecontemporaneo.it).

Ciò premesso, al fine di stabilire i presupposti per una sua legittima limitazione da parte dell'autorità pubblica, è necessario individuare il fondamento costituzionale di tale diritto. Su questo punto si fronteggiano due opinioni differenti:

- 1) secondo un primo orientamento - fatto proprio dalle Sezioni unite della Corte di Cassazione (sentenza Prisco) con riferimento al tema delle videoriprese – quando l'“intrusione” incide “solo” sulla riservatezza della vita privata, il referente costituzionale è l'art. 2 Cost., che non pone alcuna riserva di legge. La conseguenza è che l'attività investigativa atipica rientra nello schema dell'art. 189 c.p.p. e necessita unicamente del previo provvedimento dell'autorità giudiziaria (quindi anche solo del p.m.), che deve comunque essere congruamente motivato;
- 2) in base ad un secondo orientamento, invece, su tale conclusione, apparentemente lineare, è destinata ad incidere la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (C.E.D.U.), letta alla luce delle sentenze gemelle n. 348 e n. 349 del 2007 della Corte costituzionale.

Art. 8 CEDU - Diritto al rispetto della vita privata e familiare

1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.
2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

Riservatezza ex art. 8 CEDU

In forza dell'art. 8 CEDU, direttamente applicabile nell'ordinamento per effetto dell'art. 117 Cost., è oggi necessaria una legge ordinaria per consentire ingerenze dei pubblici poteri nella riservatezza della vita privata delle persone, nonostante l'art. 2 Cost. nulla dica a riguardo. Ciò perché, nell'ottica delle pronunce costituzionali nn. 348 e 349 del 2007, in questo caso è evidente il maggior livello di tutela che la fonte sovranazionale introduce rispetto a quella interna, che quindi subisce una "virtuosa" integrazione sul punto.

La conseguenza è ovvia: le perquisizioni on line incidono sul bene giuridico della riservatezza della vita privata, la cui lesione, alla luce del nuovo combinato disposto costituzionale-sovrannazionale, esige la previa determinazione, da parte del legislatore ordinario, dei casi e dei modi di aggressione di quel bene. Ergo, inammissibilità dello strumento e, comunque, inutilizzabilità degli elementi acquisiti.

Critica (1)

Secondo l'interpretazione fatta propria dalla Corte di Strasburgo, affinché un'attività di indagine sia considerata “prevista dalla legge” occorre una base di diritto interno, non importa se di natura positiva o giurisprudenziale. Ergo, le conclusioni appena esposte meritano di essere rivedute.

Critica (2)

D'altronde, anche qualora la Corte europea riscontri una violazione dell'art. 8 CEDU tale da rendere ingiustificata l'ingerenza pubblica nella sfera privata dell'individuo, ciò non comporterebbe automaticamente l'espulsione del dato illegittimamente acquisito dal materiale probatorio. La Corte, infatti, ne consente l'utilizzo al ricorrere delle seguenti tre condizioni: che quella prova risulti legittima ai sensi del diritto interno (anche se questo è stato giudicato illegittimo rispetto alla CEDU); che il dato incriminato non rappresenti l'unico elemento di cui il giudice dispone (in altre parole, sono necessari ulteriori riscontri); che non sia ritenuto determinante ai fini della condanna nel caso di specie. Ed infatti, «ritenere sempre e comunque inutilizzabili le prove assunte in violazione della Convenzione potrebbe portare, in casi estremi, a risultati difficilmente accettabili». Così, A. Tamietti, *L'utilizzazione di prove assunte in violazione di un diritto garantito dalla Convenzione non viola l'equo processo: riflessioni sul ruolo della Corte europea e sulla natura del sindacato da essa operato in margine alla sentenza P.G. e J.H. c. Regno Unito*, in *Cass. pen.*, 2002, p. 1837.

Non bisogna dimenticare, infatti, che “assicurare l'effettività della giustizia penale è considerata dalla Corte eur. come funzione essenziale dello stato, che giustifica la compressione delle garanzie individuali in misura anche maggiore di quanto non accada in altri ambiti”. Così, S. Allegrezza, *Giustizia penale e diritto all'autodeterminazione dei dati*, in AA.VV., *Protezione dei dati personali e accertamento penale*, cit., p. 74.

Dal diritto alla prassi

Nella prassi spesso accade che, pur di non rinunciare alle enormi potenzialità investigative del c.d. captatore informatico, nel silenzio del legislatore, molti pubblici ministeri hanno ritenuto opportuno, in concreto, ricorrere "analogicamente" alla disciplina delle intercettazioni per dare allo stesso una più sicura "copertura giuridica" (ed escludere eventuali eccezioni di inutilizzabilità per violazione della riserva di legge in materia probatoria).

Il caso “Bisignani”

Il fatto

Il riferimento è all'indagine sulla presunta associazione di stampo massonico P4. L'indagine fu avviata dalla Procura della Repubblica presso il Tribunale di Napoli. Secondo gli inquirenti, gli imputati avrebbero instaurato, grazie ad un'intricata rete di influenti amicizie, un sistema informativo parallelo che avrebbe avuto tra i suoi obiettivi «...l'illecita acquisizione di notizie e di informazioni, anche coperte da segreto, alcune delle quali inerenti a procedimenti penali in corso nonché di altri dati sensibili o personali al fine di consentire a soggetti inquisiti di eludere le indagini giudiziarie ovvero per ottenere favori o altre utilità».

Il caso “Bisignani”

In questo caso (siamo nel 2007), il captatore informatico era in grado, non soltanto di acquisire ed estrapolare dati ed informazioni di natura digitale memorizzati sulla memoria di massa del sistema informatico "bersaglio", ma anche di realizzare una vera e propria intercettazione ambientale, prendendo il controllo occulto del microfono e della webcam dell'elaboratore.

Il caso “Bisignani”

I sostituti procuratori incaricati delle indagini si rendono conto immediatamente della necessità di contemperare, nell'utilizzo di siffatto strumento investigativo, le esigenze investigative finalizzate all'accertamento del fatto con i diritti di difesa delle persone sottoposte ad indagine. Ed infatti, chiedono al g.i.p. di voler autorizzare, con decreto, tanto la on line search, quanto la on line surveillance, ai sensi degli art. 266 e ss. c.p.p.

Il caso “Bisignani”

Il giudice per le indagini preliminari, investito della questione, ritiene che la prima attività sia perfettamente assimilabile ad una intercettazione ambientale, seppur effettuata attraverso lo strumento atipico della "cimice informatica", e la autorizza, con decreto, a norma dell'art. 267 c.p.p. Quando alla seconda attività, egli non si discosta dal decisum della Cassazione del 2010, ritenendo sufficiente un provvedimento del P.M. a garantire le esigenze di riservatezza dei soggetti interessati

Una possibile soluzione: il principio di non sostituibilità

Applicando analogicamente le norme sulle intercettazioni al captatore informatico o, comunque, utilizzando l'art. 189 sulla prova atipica, si realizza la c.d. prova innominata o irrituale, non consentita in forza del “principio di non sostituibilità” tra mezzi di prova. Tale principio completa, unitamente alla prova incostituzionale, la materia dei divieti probatori ricavabili dal sistema: il versatile meccanismo della prova atipica non può essere utilizzato per aggirare surrettiziamente le norme del codice (ossia per superare una garanzia, un divieto o una inutilizzabilità speciale stabilita in relazione ad un differente strumento probatorio).

Cfr. C. Conti, *Accertamento del fatto e inutilizzabilità nel processo penale*, CEDAM, 2007.

Il principio di non sostituibilità nel codice di procedura penale

Di seguito, alcuni esempi del principio di non sostituibilità sparsi nel codice:

- art. 195, co. 4, sul divieto di testimonianza indiretta della polizia giudiziaria, evidentemente finalizzato ad evitare aggiramenti dell'inutilizzabilità dibattimentale delle precedenti dichiarazioni;
- artt. 202, co. 5, e 270-bis, co. 7, che vietano di acquisire indirettamente le notizie concernenti il segreto di Stato oggetto di testimonianza o di intercettazione;
- l'art. 240, co. 2, dove si legge che il contenuto dei documenti illegali non può essere utilizzato;
- l'art. 729, co. 1-ter, il quale stabilisce che non possono essere in ogni caso utilizzate le dichiarazioni, da chiunque rese, aventi ad oggetto il contenuto delle rogatorie inutilizzabili;
- l'art. 226, co. 5, disp. att., che prevede il medesimo divieto con riferimento alle intercettazioni preventive.

Il principio di non sostituibilità nel diritto vivente

Secondo la giurisprudenza di legittimità, quando il codice stabilisce un divieto probatorio oppure un'inutilizzabilità espressa, è vietato il ricorso ad altri strumenti processuali, tipici o atipici, finalizzati ad aggirare surrettiziamente un simile sbarramento.

Cass. pen., sez. un., 24 settembre 2003, Torcasio, in *Cass. pen.*, 2004, p. 30

Tale orientamento è stato progressivamente esplicitato dalla Suprema corte, la quale ha chiarito che, in presenza di limiti probatori o inutilizzabilità espresse, è vietato il ricorso ad altri strumenti processuali, tipici o atipici, che possano comunque sortire l'effetto di aggirare le norme del codice.

Cfr. Cass. pen., sez. I, 25 giugno 2009, Bellocco, in CED Cass., n. 244039; Cass. pen, sez. II, 18 marzo 2008, Fiaccambrino, ivi, n. 239746.

Il sequestro degli appunti difensivi dell'indagato (Corte cost., 18 giugno 1998, n. 229)

Il sequestro di appunti difensivi dell'indagato (predisposti al fine di prepararsi all'interrogatorio) appare “del tutto contrario alle regole del processo e direttamente lesivo di principi costituzionali. Il provvedimento si risolve in una palese diretta violazione dei diritti inviolabili della persona prima ancora che del diritto all'autodifesa [tale da] comportare, oltre tutto, una surrettizia quanto censurabile lesione delle regole dettate in tema di interrogatorio dallo stesso codice di procedura penale”.

Il c.d. “agente segreto attrezzato per il suono” (Corte cost., 30 novembre 2009, n. 320)

Con tale espressione si fa riferimento all'ipotesi in cui una persona rechi con sé apparecchi di registrazione che consentono alla polizia giudiziaria l'ascolto contestuale o differito di una conversazione. Ebbene, secondo la Consulta, quantomeno in ipotesi di ascolto contestuale, la presenza di un “terzo orecchio” occulto ad almeno uno degli interlocutori lede la segretezza della comunicazione. Pertanto, la soluzione preferibile consiste nel considerare l'atto alla stregua di un'intercettazione. Una differente interpretazione –nell'ottica della Consulta- comporterebbe l'elusione delle garanzie stabilite dal codice.

Il sequestro della corrispondenza del detenuto (Cass. pen., sez. VI, 10 dicembre 2009, Giacalone e sez. II, 23 giugno 2006, Rescigno)

E' il caso del pubblico ministero che, all'insaputa dell'interessato, ordina all'amministrazione penitenziaria di consegnare la corrispondenza del detenuto alla polizia, a sua volta incaricata di estrarne copia. Successivamente, le buste vengono richiuse ed inoltrate al destinatario, mantenuto all'oscuro di siffatta attività. Si tratta di un provvedimento che realizza una parziale fusione di due atti tipici (il sequestro di corrispondenza ex art 353 ed il visto di controllo sulla corrispondenza del detenuto, disciplinato dall'art. 18-ter ord. pen.), dando vita ad un ibrido *terzium genus* che finisce per eludere le garanzie tipiche di entrambi.

Inoltre, la possibilità di applicare in via analogica all'attività in esame la disciplina delle intercettazioni è stata esclusa dalle Sezioni unite, udienza camerale del 19 aprile 2012, ricorrente Pasqua.

CONCLUSIONI

Nel caso specifico del captatore informatico, l'utilizzo dei virus trojan per fini investigativi desta perplessità in ragione della eterogenea moltitudine di informazioni -di carattere "comunicativo", ma anche "non comunicativo"- potenzialmente estrapolabili attraverso questo nuovo strumento tecnologico.

Informazioni “comunicative”

Quanto alle informazioni qualificabili come "comunicazioni" e ottenibili attraverso il virus, la copertura giuridica offerta dagli artt. 266-bis e ss. del codice di rito tiene ma ciò non ci esenta dalle seguenti considerazioni critiche:

- l'attività dei tecnici sfugge, per sua natura, al controllo dell'autorità giudiziaria e della stessa p.g.;
- non è necessaria alcuna "collaborazione tecnica" ulteriore da parte del gestore telefonico, con la conseguenza che l'attività di *remote forensics* è totalmente nelle mani del tecnico ausiliario di p.g.

Informazioni “non comunicative”

Elusione delle seguenti garanzie difensive previste per le perquisizioni tradizionali:

- conoscibilità dell'atto (250);
- assistenza del difensore (365);
- deposito del verbale (366);
- adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione (247, co. 1-bis).

Il caso “Ryanair” (Cass. pen., Sez. IV, 17 aprile 2012 n. 19618)

Il fatto

Il P.M. aveva disposto il sequestro e la perquisizione delle credenziali di accesso al sistema di *booking online* di una nota compagnia aerea, motivando il provvedimento sulla base dell'esigenza investigativa di identificare in tempo reale i passeggeri sospettabili di fungere da corrieri internazionali di sostanze stupefacenti (c.d. ovulatori)

Il caso “Ryanair” (Cass. pen., Sez. IV, 17 aprile 2012 n. 19618)

Il diritto

I mezzi di ricerca della prova, nessuno escluso, non possono prescindere dalla previa acquisizione di una qualificata notizia di reato, non essendo consentito, nel nostro ordinamento giuridico, utilizzare uno strumento atipico con finalità esplorative, di tipo preventivo.

Coerentemente con tale collocazione, per l'emissione del provvedimento è richiesta la forma del decreto motivato che deve necessariamente contenere l'indicazione della fattispecie concreta nei suoi estremi essenziali di tempo, luogo e azione nonché della norma penale che si intende violata, non essendo sufficiente la mera indicazione del titolo di reato

Il caso “Ryanair” (Cass. pen., Sez. IV, 17 aprile 2012 n. 19618)

Conseguenza

La Cassazione ha rigettato il ricorso promosso dalla Procura contro l’ordinanza di annullamento emessa dal Tribunale del Riesame.

Qualora si consentisse diritto di cittadinanza a tale strumento processuale – si è osservato – «si verrebbe [...] ad integrare un nuovo ed anomalo strumento di ricerca della prova, con finalità nettamente esplorative, di mera investigazione (paragonabile alle intercettazioni), che nulla ha a che fare con la perquisizione»

In conclusione, dunque, de iure condito sembra doversi trarre il divieto di utilizzare i virus informatici sia nell'ambito delle indagini atipiche sia mediante l'impiego della disciplina delle intercettazioni: è di ostacolo il principio di non sostituibilità, che deriva da una esegesi puntuale delle stesse norme del codice di rito, all'indomani della novella del 2008. Al fine di acquisire dati utili all'accertamento processuale –e nei limiti in cui, anche sotto un profilo tecnico, ciò sia possibile– è necessario ricorrere anche cumulativamente alle attività tipiche o atipiche consentite.

Per il resto, ci è caro ricordare un insegnamento antico ma ancora attuale, in base al quale, «allo Stato e alla comunità internazionale [...] compete [...] il compito di disciplinare l'uso dei progressi tecnici entro rigorosi schemi giuridici» .

G. VASSALLI, *La protezione della sfera della personalità nell'era della tecnica*, in AA.VV., *Studi in onore di Emilio Betti*, vol. V, Giuffrè, Milano, 1962, p. 684.

Bundesverfassungsgericht del 27 febbraio 2008

Il fatto

L'art. 5, comma 2, n. 11 della legge sulla protezione della Costituzione del Nord Reno-Westfalia consentiva ad un organismo di intelligence di derivazione governativa il monitoraggio e l'accesso segreto ai sistemi informatici collegati in rete. In pratica, la norma in argomento avrebbe garantito ai servizi segreti del Nord Reno-Westfalia il diritto di cercare ed intercettare in modo occulto comunicazioni via internet, nonché la possibilità di accedere segretamente a qualsiasi sistema informatico collegato in rete

Bundesverfassungsgericht del 27 febbraio 2008

Il diritto

La Corte tedesca ha affermato l'esistenza di un nuovo diritto costituzionale alla riservatezza ed alla integrità dei sistemi informatici. Così come il diritto all'autodeterminazione informativa, questo nuovo diritto fondamentale viene fatto derivare dall'art. 1.1 della Costituzione tedesca, il quale dispone che «la dignità umana è inviolabile e tutti gli organi dello Stato hanno l'obiettivo finale di proteggerla»

Bundesverfassungsgericht del 27 febbraio 2008

Il diritto

Secondo la Corte, il ricorso a nuove forme di investigazione tecnologica non è di per sé contrario a Costituzione. Tuttavia, la loro regolamentazione, a livello legislativo, e la loro utilizzazione, a livello esecutivo, non possono non tener conto del bilanciamento con eventuali interessi contrapposti, a partire dai diritti fondamentali dell'individuo.

Questo si traduce, per il legislatore, a livello di tecnica normativa, nell'obbligo del rispetto dei principi di:

- chiarezza e sufficiente determinatezza della fattispecie

- Proporzionalità: una legge che preveda la compressione di diritti fondamentali deve perseguire uno scopo legittimo e ben individuato, e deve essere idonea ed opportuna quale mezzo per il raggiungimento di tale fine. Secondo la Corte, unico scopo che possa giustificare l'accesso ed il monitoraggio segreto su Internet è la necessità di proteggere importanti e predominanti beni giuridici, quali la vita, l'incolumità fisica e la libertà dei singoli, la cui minaccia tocca le fondamenta di uno Stato di diritto. Di conseguenza, la compressione di diritti fondamentali nel contesto di un generico obiettivo di prevenzione (come era, nel caso di specie) non soddisfa il principio di proporzionalità (adeguatezza).

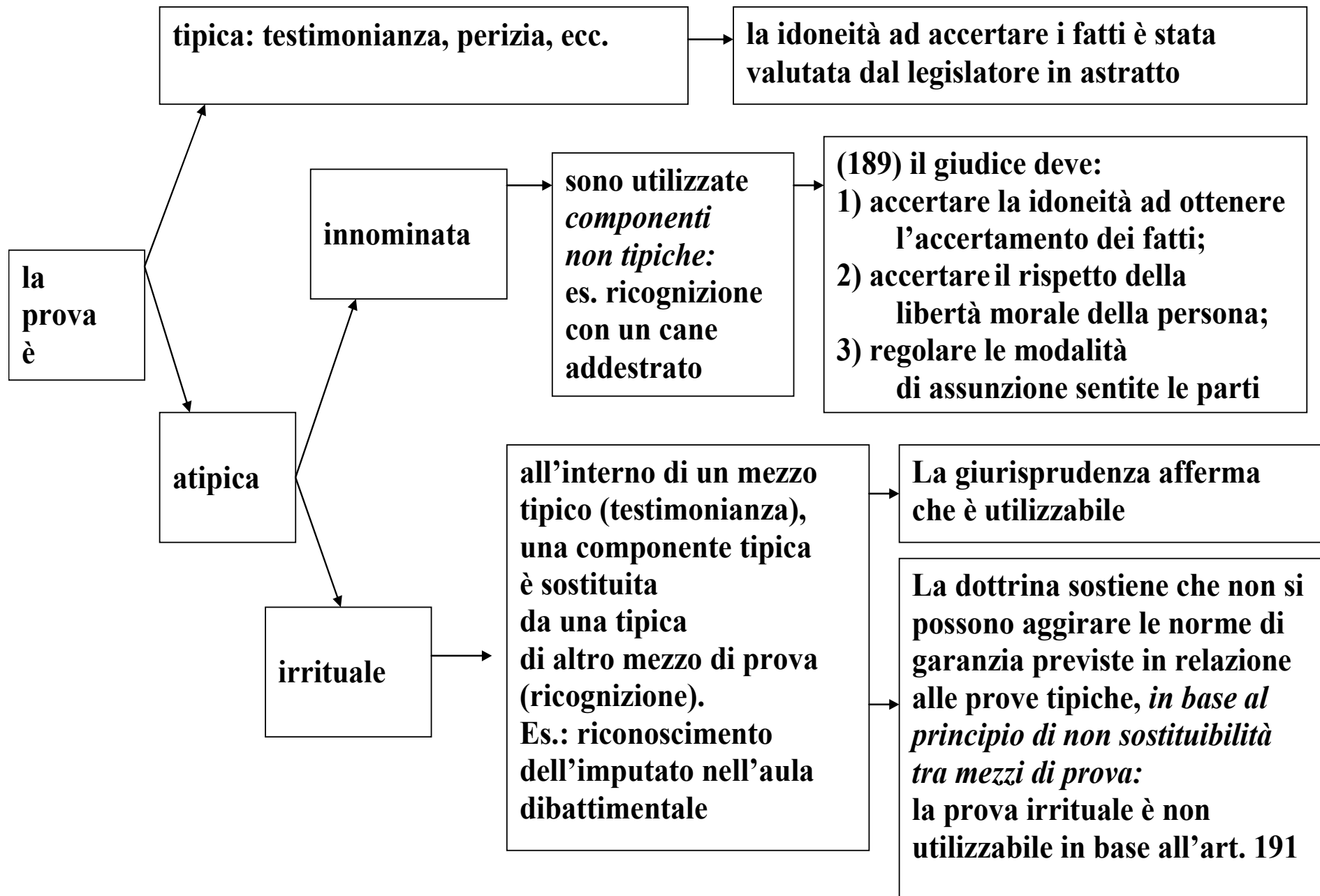
Bundesverfassungsgericht del 27 febbraio 2008

P.Q.M.

La Corte costituzionale tedesca ha ritenuto il par. 5, comma 2, n. 11 del VSG non conforme ai principi di chiarezza, determinatezza e proporzionalità in senso stretto, dichiarandolo incostituzionale. «La declaratoria di incostituzionalità non riguarda, pertanto, i nuovi mezzi "di carattere tecnologico" in quanto tali ed in termini assoluti, ma (i loro modi di utilizzo) i presupposti ed i limiti, anche temporali, per la loro adozione, secondo i principi che deve seguire il legislatore nel formulare la norma, oltre che la mancata riserva, in ordine alla verifica sulla sussistenza di simili presupposti, ad un organismo indipendente e neutrale. In altre parole il legislatore avrebbe dovuto determinare i casi, le finalità ed i confini della compressione del diritto fondamentale, in modo da rendere chiara e precisa, in termini di formulazione legislativa, la "zona" di intervento -riferita a gravi reati a tutela di importanti beni giuridici- nel rispetto del principio di proporzionalità, nonché prevedere quella riserva all'autorità giudiziaria». Così, R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung.*

In Italia: decreto legge 18 febbraio 2015, n. 7 (c.d. decreto legge antiterrorismo)

Art. 2, comma 1-ter: “al codice di procedura penale sono apportate le seguenti modificazioni: a) all’art. 266-bis, comma 1 (“1. 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” sono aggiunte le seguenti parole: “, **anche attraverso l’impiego di strumenti e di programmi informatici per l’acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico**”.



2.4.1. Mezzi di prova atipici

2.5.9.
Videoriprese

Attraverso strumenti tecnici di captazione viene registrato quanto accade in un luogo all'insaputa di chi in esso si trovi

Videoripresa effettuata
da soggetti pubblici

Videoripresa effettuata
da soggetti privati

Comportamenti non comunicativi

Comportamenti comunicativi
(dialoghi e immagini):
è intercettazione

è utilizzabile
se non
viola
divieti
probatori

è documento
illegale
se
effettuato
con
violazione
delle
norme
penali
sulla
privacy
(240.2)

In luogo
pubblico

In luoghi "riservati"
(es. *toilette* di un
locale pubblico):
lo *ius excludendi alios*
esiste soltanto in
presenza del soggetto
nel luogo

Nel domicilio:
lo *ius excludendi alios*
esiste anche
in assenza del
soggetto nel luogo

In luoghi pubblici
o riservati

Nel domicilio

è prova
atipica
disposta dalla
polizia
giudiziaria:
è ammessa in
dibattimento
e il giudice
deve sentire le
parti sulle
modalità di
acquisizione
(189) (SU
2006)

è utilizzabile
come prova
atipica (art. 189
c.p.p.),
purché sia
autorizzata con
provvedimento
motivato del PM.
È applicabile
l'art. 2 Cost.:
non vi è riserva di
legge e di
giurisdizione sui
casi e modi (SU
2006)

In concreto il
comportamento è
"non riservato"
(es. finestra
aperta) e la
ripresa avviene
senza l'impiego
di strumenti
che superano
la normale
accessibilità ai
terzi (es. no
zoom) (C.cost.
149/2008)

Il
comportamento
è "riservato"

è interce-
tazione
ordinaria
(266.1):
autorizzata
se vi sono
gravi indizi

è intercettazione
ambientale (266.2):
autorizzata se vi sono
gravi indizi
e se vi è fondato
motivo di ritenere
che nel domicilio si
stia svolgendo
attività criminosa

la ripresa deve considerarsi vietata in assenza
di una espressa regolamentazione legislativa dei
casi e modi di tale apprensione (191).

Ciò è imposto dall'art. 14 Cost. sulla
inviolabilità del domicilio (riserva di legge e di
giurisdizione) (SU 2006 e C. cost. 149/2008)

Aggiornamento a P. TONINI,
*Manuale breve. Diritto
proc. penale* ed. Giuffrè,
Milano, 2008