

ORIENTAMENTI

SERGIO COLAIOCCO

Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia

SOMMARIO: 1. Sistemi informatici e telematici. - 2. Intercettare il flusso telematico di dati. - 3. Captare il contenuto di un sistema informatico. - 3.1 Perquisizioni. - 3.2 Ispezioni. - 4. La pronuncia della Corte di Cassazione. - 5. La prova atipica secondo le sezioni unite. - 6. Conclusioni.

1. La tecnologia informatica permette, da qualche anno, forme d'intrusione particolarmente invasive della sfera privata dell'indagato.

Grazie all'utilizzo di "programmi spia", denominati anche "*trojan*", è possibile, come noto, monitorare sia il flusso di comunicazioni riguardanti sistemi informatici o telematici, sia monitorarne il contenuto.

Preliminarmente appare utile chiarire cosa si debba intendere, dal punto di vista giuridico, per sistema informatico o telematico.

In assenza di una definizione legislativa, era stata la giurisprudenza a tentare di fornire una definizione generale di sistema informatico in forza della quale doveva reputarsi tale ogni apparecchiatura più o meno complessa "destinata a svolgere qualsiasi funzione utile all'uomo attraverso l'utilizzazione, anche solo parziale, di tecnologie informatiche"¹.

Si trattava di una definizione incentrata sul passaggio dal "dato" all'"informazione"; nel senso che alla funzione di registrazione-memorizzazione elettronica di dati, intesi quali rappresentazioni elementari di un fatto, si affianca la funzione di elaborazione-organizzazione logica di tali dati in insiemi più o meno estesi costituenti "informazioni".

L'attitudine della macchina (*hardware*), a organizzare ed elaborare dati in conformità a un certo programma (*software*) e in vista di finalità eterogenee costituisce elemento discrezionale essenziale, consentendo di distinguere ciò che è informatico da ciò che è invece solamente elettronico².

¹ Queste ultime sono caratterizzate dalla compresenza di tre aspetti funzionali: a) la registrazione o memorizzazione, "per mezzo di impulsi elettronici e su supporti adeguati, di dati rappresentati attraverso simboli (*bit*) numerici (codice) in combinazioni diverse"; b) "l'elaborazione automatica" da parte della macchina dei dati così registrati o memorizzati; c) l'organizzazione di tali dati "secondo una logica che consenta loro di esprimere un particolare significato per l'utente" (utilità). In tal senso vedi per maggiori approfondimenti STALLA, *L'accesso abusivo ad un sistema informatico o telematico*, in *www.penale.it*, o per la giurisprudenza Cass., Sez. VI, 4 ottobre 1999, Piersanti, in *Cass. pen.*, 2000, 1611, con nota di ATERNO.

² Così, ad esempio, il videoregistratore, il lettore di CD (sempre che non siano connessi ad un computer con funzione di masterizzazione o elaborazione di immagini e suoni), i dispositivi che presiedono

Più sistemi informatici collegati stabilmente tra loro, per esempio via modem o anche via radio se connessi con tecnologia *wireless* al fine di permettere la trasmissione-comunicazione a distanza delle informazioni raccolte costituiscono un sistema telematico.

In tal caso l'elemento che consente di ravvisare un sistema telematico in luogo di un mero dispositivo di trasmissione a distanza di segnali, come il telefono o il fax, è dato proprio dal fatto che a essere collegati tra loro, sono due o più sistemi informatici.

L'orientamento della giurisprudenza ha trovato, in seguito, conferma nell'art. 1 della Convenzione europea di Budapest del 2001 che ha consacrato la definizione di sistema informatico come «*qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati*»³.

Si tratta di definizioni molto ampie, suscettibili di ricomprendere tanto l'*hardware* quanto il *software*, tanto la macchina nel suo insieme, quanto le sue singole parti, a condizione che il tutto sia unitariamente finalizzato all'espletamento di quelle funzioni e al raggiungimento di quelle utilità.

Rientrano dunque nella nozione il più piccolo *personal computer* come anche il supercalcolatore capace di gestire un numero indeterminato di utenti simultaneamente a esso collegati via terminale; la rete locale di realtà aziendali o professionali, così come la grande rete⁴.

Orbene, il monitoraggio di un sistema informatico o telematico, così definiti, attraverso l'utilizzo di "programmi spia", ha due peculiarità rilevanti; in primis, che esso non provoca alcuna interferenza qualitativa sulle prestazioni rese dal dispositivo interessato, sia esso un computer o una connessione internet. In secondo luogo, e proprio in conseguenza di quanto detto, il destinatario nulla può sospettare del monitoraggio in corso giacché avviene in modalità silente.

A livello tecnico, esistono essenzialmente due modelli di monitoraggio: la *online surveillance* ovvero la *cd online search* o *one time copy*. La prima

all'attivazione dei sistemi di sicurezza sulle auto (come l'airbag, o l'ABS), certi elettrodomestici a tecnologia digitale sempre più diffusi nelle nostre case, non possono considerarsi - proprio perché inidonei alla elaborazione ed organizzazione di dati nel senso che si è detto - "sistemi informatici", quanto solamente apparati elettronici.

³ Così recita l'art. 1 della Convenzione europea di Budapest del 23 novembre 2001: «*Computer system*" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data».

⁴ Per ulteriori approfondimenti vedi GIANNANTONIO, *L'oggetto giuridico dei reati informatici*, in *Cass. pen.*, 2001, 2029; PATERNA, «New economy» e «cybercrimine», in *Crimin. psic. for.*, 2000, 16, 50; DI GIANDOMENICO, CUOMO (a cura di), *Profili giuridici dell'informatica*, Napoli, 2000.

permette un monitoraggio costante delle attività in rete compiute, in entrata o in uscita, da un dispositivo informatico; la seconda si caratterizza per consentire l'acquisizione, mediante copia, di dati contenuti all'interno delle memorie di un dispositivo informatico, nella maggior parte dei casi un personal computer.

Evidenti sono le potenzialità di siffatti strumenti investigativi nell'accertamento di fatti-reato soprattutto nell'ambito delle indagini preliminari. Potenzialità intrusiva che comportando una forte limitazione dei diritti fondamentali dell'indagato (artt. 2 e 14 della Cost.) deve, però, trovare la sua legittimazione in un ben definito quadro giuridico di riferimento.

Il percorso logico-giuridico che ci apprestiamo a percorrere non può che partire, allora, dalla distinzione tra le due peculiari ed originali funzioni che i "programmi spia" svolgono: quella di captare il flusso telematico di dati (c.d. *online surveillance*) e quella di captare il contenuto di un sistema informatico (c.d. *online search* o *one time copy*). Ciò in quanto, per ognuna delle due diverse funzioni, sarà necessario verificare la conformità dello strumento investigativo a uno degli atti d'indagine tipizzati dal codice di procedura. Qualora detta ricerca si riveli infruttuosa occorrerà verificare, in subordine, se l'atto d'indagine possa almeno rientrare nella categoria delle cosiddette prove atipiche previste dall'art. 189 c.p.p.

2. Orbene, partendo dall'*online surveillance*, deve osservarsi come nell'ambito di questa definizione è inquadrata ogni attività di monitoraggio che abbia a oggetto il flusso di dati trasmesso da una sistema informatico a un altro. Tipicamente rientra in questa captazione il flusso telematico che si genera, ad esempio, quando si utilizza la rete d'*internet*; in essa rientrano la captazione delle conversazioni originate dal *software skype*, tutte le *chat*, le *mail*, gli sms o mms.

Tale mezzo di ricerca della prova è tipizzato nell'art. 266-*bis* c.p.p. che consente la captazione, o in altri termini il controllo continuo, del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi.

È, quindi, possibile porre in essere siffatta attività con le garanzie previste dall'art. 266 e ss. c.p.p. come ribadito anche dalla Corte di Cassazione che ha affermato come «*l'intercettazione di flussi telematici riconducibili a un determinato utente mediante la procedura di monitoraggio del percorso, disposta dal G.I.P., comporta la legittima captazione dei flussi informatici*

gestiti dal soggetto»⁵.

Si osservi. Presupposti essenziali per ricondurre le attività investigative di captazione all'art. 266-*bis* sembrano essere due: la circostanza che si sia alla presenza di flussi e, in secondo luogo, che i flussi intercorrano tra due dispositivi informatici.

Quanto al primo aspetto esso delimita il perimetro entro il quale lo strumento investigativo dell'*online surveillance* è ristretto; è, infatti, solo il dato dinamico che può essere oggetto d'intercettazione con le procedure di cui all'art. 266-*bis* c.p.p. e, quindi, il flusso dei dati da un sistema informatico a un altro; in altri termini ciò che è esclusa è l'acquisizione di dati contenuti in una memoria poiché non costituiscono oggetto di trasmissione attraverso dispositivi informatici.

In relazione, invece, alla necessità che i flussi intercorrano proprio e solo tra due dispositivi informatici, deve qui meglio specificarsi quanto detto in apertura circa la differenza tra sistemi elettronici e sistemi informatici; il discrimine, come detto, è l'idoneità dei soli dispositivi informatici a effettuare un'elaborazione-organizzazione logica di tali dati.

Ebbene, questione aperta a tal proposito è quella relativa all'inquadramento tra i sistemi informatici di alcuni dispositivi accessori di necessario o comunque frequente utilizzo: la tastiera e la stampante. Infatti solo qualora detti apparecchi siano classificati come dispositivi informatici sarà captabile il flusso di dati che il dispositivo centrale riceve dalla tastiera e che, eventualmente poi, dal dispositivo centrale sia inviato alla stampante. In caso negativo, e forti perplessità desta soprattutto l'inquadramento della tastiera quale dispositivo informatico (al più solo quelle dotate di "*bluetooth*" sembrano riconducibili all'ambito informatico), la captazione in parola dovrebbe trovare diversa copertura. Ciò in quanto nell'ipotesi in cui si sia alla presenza di un unico sistema informatico non ricorre il presupposto dell'esistenza di una situazione dinamica cioè di un flusso di dati tra più sistemi come richiesto dall'art. 266-*bis* c.p.p. che consente solo «*l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi*».

3. Passando a esaminare la c.d. *online search* o *one time copy* detta attività si caratterizza per l'acquisizione mediante copia di dati contenuti all'interno

⁵ Vedi, *ex plurimis*, Cass., Sez. I, 14 febbraio 2005, Palamara, in *Mass. Uff.*, n. 231591, che sembra aver accolto una interpretazione ampia del termine "comunicazioni" dell'art. 266-*bis* così ricomprendendo non solo lo scambio di informazioni sincrono o asincrono tra due utenti persone fisiche ma anche lo scambio tra un utente e dispositivo informatico quale ad esempio una banca dati, un *cloud* ecc.

delle memorie di un dispositivo informatico. In siffatta ipotesi il primo riferimento, trattandosi di un'acquisizione di una *res* dell'indagato, non può che esser fatto alle perquisizioni tradizionali. Tra l'altro, proprio per l'immediatezza del riferimento di questa funzione dei *programmi spia* alla perquisizione, lo strumento investigativo in parola è, spesso, definito quale "perquisizione on line"⁶.

3.1. Emergono però subito molteplici punti di divergenza, che non consentono di ricondurre quest'ultime alla disciplina tipica (artt. 247 e ss. c.p.p.). Le perquisizioni, infatti, sono ontologicamente indirizzate alla ricerca del corpo del reato e delle cose pertinenti al reato che, in caso di ritrovamento, devono essere necessariamente sequestrate; l'utilizzo di programmi spia, o in altri termini le c.d. perquisizioni *on line*, invece, prescindono dalla ricerca del corpo del reato e/o delle cose pertinenti al reato e non sfociano necessariamente in un sequestro.

Ciò non bastasse, si deve osservare come le perquisizioni tradizionali sono atti a sorpresa nel senso che se non deve essere dato previo avviso del loro compimento all'indagato, quest'ultimo, ove presente, ben si accorge, durante lo svolgimento delle operazioni, di essere sottoposto all'atto coercitivo, tanto da avere diritto ad una serie di adempimenti in funzione garantistica (notifica del decreto motivato, invito a nominare un difensore di fiducia ovvero, in mancanza, designazione di un difensore d'ufficio, conseguente diritto di farsi assistere dal difensore).

Le perquisizioni *on line*, invece, non sono solamente atti a sorpresa ma, per essere fruttuose, devono restare ignote all'indagato durante tutto il corso del loro svolgimento.

Né le novità introdotte dalla legge n. 48 del 2008 possono far giungere a diverse conclusioni. Infatti, anche quando hanno per oggetto sistemi informatici o telematici, le perquisizioni "tradizionali" non vengono meno alla loro finalità di ricerca di cose pertinenti al reato e rimangono comunque

⁶ Per approfondimenti vedi: MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, 2855; BONO GAETANO, *Il divieto di indagini ad explorandum include i mezzi di ricerca della prova*, in *Cass. pen.*, 2013, 1525. MOLINARI, *Questioni in tema di perquisizioni e sequestro di materiale informatico*, in *Cass. pen.*, 2012, 696; DANIELE, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen.*, 2013, 367. *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, a cura di Luparia, Milano, 2012; ATERNO, CAJANI, COSTABILE, MATTIUCCI, MAZZARACO, *Manuale di Computer Forensics*, Forlì, 2012; ATERNO, voce *Digital Forensics*, in *Dig. Pen.*, Padova, p. 58, in corso di pubblicazione ed infine Aterno, Mattiucci, *Cloud Forensics e nuove frontiere delle indagini informatiche nel processo penale*, in *questa Rivista*, 2013, 865 ss.

garantite dagli ordinari diritti difensivi appena sopra menzionati⁷.

3.2. Ad analoghe conclusioni sembra doversi pervenire per quanto concerne un altro mezzo di ricerca della prova tipico: le ispezioni. Secondo la dottrina e la giurisprudenza, la differenza tra perquisizioni e ispezioni è costituita dal fatto che le prime sono finalizzate alla ricerca di determinati oggetti, corpo del reato o cose pertinenti al reato, mentre le ispezioni sono volte a fotografare una situazione di fatto suscettibile di modifica (artt. 244 ss. c.p.p.). Né il quadro è mutato per effetto delle modifiche introdotte dalla legge n. 48 del 2008, che si è limitata a contemplare, all'art. 244, co. 2, c.p.p., anche i sistemi informatici e telematici come possibili oggetti d'ispezione, ma senza mutare la natura genetica dell'atto ispettivo. Viceversa, l'introduzione di un programma spia risulta totalmente estranea alla funzione descrittiva, tipicamente statica, delle ispezioni, essendo atto a una "subdola" raccolta, anche prolungata nel tempo, di dati e informazioni di pertinenza dell'indagato, a sua insaputa. Da ciò discende l'inadeguatezza delle garanzie legali previste: ai sensi dell'art. 364 c.p.p., l'ispezione è normalmente sottoposta a termini di preavviso (co. 1) e, anche nei casi di maggior urgenza, è sempre «*fatta salva [...] la facoltà del difensore d'intervenire*» (co. 5): facoltà che presupporrebbe una *discovery* che vanificherebbe del tutto gli scopi di qualsiasi perquisizione *on line*⁸.

4. Esclusa per quanto sopra la riconducibilità dell'utilizzo dei programmi spia – quando sono utilizzati per l'acquisizione mediante copia di dati contenuti all'interno delle memorie di un dispositivo informatico – a un tipico mezzo di ricerca della prova, non resta che volgere lo sguardo all'art. 189 c.p.p. per verificare l'accessibilità di siffatto atto d'indagine al processo penale.

Orbene non si può non partire, nel verificare se l'uso dei cosiddetti programmi spia rientri nel quadro previsto dall'art. 189 c.p.p., dall'unica sentenza di legittimità che sinora ha affrontato la questione⁹.

La Corte di Cassazione, infatti, ha catalogato tra le prove atipiche l'impiego di un *trojan* da parte dell'Autorità Giudiziaria per finalità investigative e in grado, all'epoca dei fatti, solo di introdursi all'interno di un personal computer e di acquisire da remoto tutto il suo contenuto.

⁷ Vedi anche Cass., Sez. IV, 24 maggio 2012, Soc. Ryanair, in *Mass. Uff.*, n. 252689, ove si esclude la riconducibilità alla perquisizione di una attività che è mirata ad acquisire dati non presenti nel sistema informatico al momento in cui l'atto viene disposto.

⁸ Vedi in tal senso MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, 2855.

⁹ Vedi Cass., Sez. V, 29 aprile 2010, Virruso, in *Mass. Uff.*, n. 246955.

Il fatto storico sul quale si è pronunciata la Suprema Corte trae origine dall'attività d'indagine disposta dal Pubblico Ministero - con un decreto di acquisizione di atti ai sensi dell'art. 234 c.p.p. - su un *personal computer* di un ente pubblico utilizzato da uno degli indagati.

Il decreto ha disposto la registrazione non solo dei *files* esistenti, ma anche dei dati che sarebbero stati inseriti in futuro nel *personal computer*, in modo da acquisirli periodicamente. Le concrete modalità esecutive del decreto, consistite nell'installazione, all'interno del sistema operativo del *personal computer*, di un captatore informatico erano in grado di memorizzare i *files* già esistenti e di registrare in tempo reale tutti i *files* elaborandi, innescando in tal modo un monitoraggio occulto e continuativo del sistema informatico.

Nella specie, l'attività autorizzata dal Pubblico Ministero era consistita nel prelevare e copiare documenti memorizzati sull'*hard disk* dell'apparecchio in uso all'indagato che lavorava negli uffici di un Comune e 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"¹⁰, ossia ad attività confinate all'interno dei circuiti del personal computer.

Per queste ragioni la Corte ha ritenuto di poter ricondurre l'attività di captazione in questione al concetto di prova atipica con conseguente utilizzo dei risultati.

La Corte ha esaminato anche ad altre eccezioni affermando come l'attività captativa non avesse violato gli articoli 14 e 15 della Costituzione.

Secondo i supremi giudici l'apparecchio monitorato con l'installazione del captatore informatico non era collocato in un luogo di privata dimora, ancorché intesa nella sua più ampia accezione, bensì in un luogo aperto al pubblico. Il personal computer, infatti, si trovava nella locale sede di un ufficio pubblico comunale, ove sia l'indagato sia gli altri impiegati avevano accesso per svolgere le loro mansioni e ove potevano fare ingresso, sia pure in determinate condizioni temporali, il pubblico degli utenti e il personale delle pulizie, insomma una comunità di soggetti non particolarmente estesa, ma nemmeno limitata o determinabile a priori in ragione di una determinazione personale dell'indagato. D'altra parte, nel caso di specie, non poteva essere invocata la tutela costituzionale della riservatezza della corrispondenza e in genere delle comunicazioni, giacché quanto riprodotto in copia, non era un testo inoltrato e trasmesso col sistema informatico privato e personale, ma

¹⁰ Vedi Cass., Sez. V, 29 aprile 2010, Virruso, cit.

«soltanto predisposto per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario»¹¹.

In conclusione, in questa sentenza del 2010 la Suprema Corte ha ritenuto legittimo il decreto del pubblico ministero di acquisizione, in copia, della documentazione informatica memorizzata nel personal computer in uso all'imputato in un ufficio pubblico attraverso l'installazione di un captatore informatico. Siffatta scelta si è basata sulla circostanza che il provvedimento ha riguardato l'estrapolazione di dati e non un flusso di comunicazioni già contenute nella memoria del personal computer, e ha ritenuto corretta la qualificazione dell'attività di captazione quale prova atipica sottraendola alla disciplina prescritta dagli artt. 266 ss. c.p.p.

Limitata, secondo molti commentatori, appare l'applicabilità della pronuncia in esame per un dato fattuale decisivo e, cioè, che il sistema informatico era collocato ed utilizzato in un ufficio pubblico; circostanza questa che ha permesso alla Corte Suprema, dopo aver superato positivamente lo scrutinio di rispondenza ai requisiti dall'art. 189 c.p.p., di evitare di dover affrontare i problemi relativi alla compatibilità dello strumento investigativo in esame con i parametri costituzionali e sovranazionali in tema di tutela della riservatezza e del domicilio.

Secondo un recente orientamento di merito tali perplessità possono ritenersi superate dai progressi tecnologici successivi alla sentenza della Suprema Corte. Ciò in quanto, a differenza del 2004, anno del quale sono i fatti esaminati dai giudici di legittimità, è oggi diventato possibile introdurre in un dispositivo informatico un programma spia a distanza anche tramite la rete internet.

Secondo siffatto orientamento in tale caso non si porrebbe il problema della riservatezza del domicilio di cui all'art. 14 Cost., che sarebbe violato, da parte della P.G., solo in caso d'installazione tramite accesso presso la privata dimora ove il dispositivo informativo da monitorare è collocato.

Di conseguenza inserendo il virus da remoto non sarebbe effettuato alcun accesso o intrusione fisica nel luogo ove si trova il dispositivo da monitorare, sicché non avrebbe senso una distinzione fra quei dispositivi installati in luoghi di privata dimora e quelli collocati in luogo pubblico.

Orbene il pur suggestivo orientamento su richiamato non sembra esser sostenuto da un adeguato supporto argomentativo.

Sembra, infatti, utile ricordare come il legislatore, sin dal 1993, ha introdotto accanto al domicilio "fisico" una nuova figura, quella del cosiddetto domicilio

¹¹ Vedi Cass., Sez. V, 29 aprile 2010, Virruso, cit.

informatico, ove si esplica oramai buona parte delle attività quotidiane degli individui e ove ognuno esprime, quindi, la propria personalità con la conseguente facoltà di escludere i terzi non graditi.

In quest'ottica i sistemi informatici costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli artt. 614 e 615 del codice penale¹².

Non a caso le fattispecie incriminatici in tema di criminalità informatica introdotte con la legge n. 573 del 1993 sono state inserite tra quelle a tutela della libertà di domicilio. Anche recentemente il giudice nomofilattico ha confermato che il progresso tecnologico ha determinato l'insorgere di nuovi luoghi di espressione della personalità dell'individuo tra cui vi è senz'altro il sistema informatico all'interno del quale il soggetto conserva dati personali la cui diffusione ha diritto ad impedire e a controllare l'utilizzo dei dati inseriti in banche dati.

L'art. 615-ter c.p. individuando uno spazio virtuale definibile come domicilio informatico, ha riconosciuto e tutelato il diritto di un soggetto ad impedire la diffusione incontrollata e non gestita di informazioni che lo riguardano. Tale spazio acquista, quindi, una sua entità propria che lo separa dall'esterno e grazie all'esercizio dello *ius excludendi* è possibile accedervi solo attraverso altre informazioni, come le chiavi logiche di accesso, o comunque superando le misure di sicurezza¹³.

Per queste ragioni sembra che la tecnica attraverso cui il programma spia è collocato nel dispositivo, circostanza che è assunta come determinante secondo l'orientamento qui non condiviso, non tenga alcun conto del fatto che oggi le tutele riconosciute al domicilio fisico sono riconosciute anche al domicilio informatico con piena equiparazione delle garanzie.

Ciò detto, in realtà sembra che anche la pronuncia della Suprema Corte, Virruso, del 2010 innanzi citata susciti perplessità che investono primariamente altro profilo che appare di particolare pregnanza; difatti la sentenza Virruso sembra aver disatteso la linea interpretativa in tema di prova atipica fatta propria dalle Sezioni Unite del 2006, concernente le riprese visive nel domicilio.

5. Nella nota sentenza “Prisco” delle Sezioni Unite del 2006 la Corte di Cassazione, nell'affrontare la questione delle riprese video nei luoghi di

¹² Relazione sul disegno di legge n. 2773, che successivamente ha dato origine alla legge n. 547 del 1993.

¹³ Vedi Cass., Sez. V, 18 dicembre 2012, Valenza, in *Mass. Uff.*, n. 255924.

privata dimora, ripercorre il dibattito dottrinale e i diversi orientamenti giurisprudenziali di legittimità in ordine alle cd. prove incostituzionali in relazione all'art. 189 c.p.p.

Secondo la Corte non occorre, però, per giungere alla conclusione che non possono considerarsi ammissibili, come prove atipiche, le prove acquisite in violazione dell'art. 14 Cost., né prendere posizione sul dibattito relativo agli effetti che la violazione delle norme costituzionali di garanzia può avere sull'attività probatoria prevista dal codice di rito, né stabilire se la sanzione dell'inutilizzabilità attenga solo alla violazione dei divieti stabiliti dalla legge processuale o riguardi anche la violazione di norme costituzionali o di altri rami dell'ordinamento, e segnatamente di quello penale.

Afferma infatti la Suprema Corte: «(...) a ben vedere questi aspetti controversi non vengono in questione perché la soluzione passa direttamente attraverso l'interpretazione dell'art. 189 c.p.p., che è stato richiamato per legittimare processualmente l'attività probatoria "incostituzionale". Si vuole dire che il tema della inutilizzabilità come sanzione processuale per la violazione di regole di rango costituzionale riguarda, in linea di principio, le prove tipiche e non quelle atipiche. Prima dell'ammissione le prove atipiche non sono prove, perciò se sorge questione sulla legittimità delle attività compiute per acquisire i materiali probatori che le sorreggono ci si deve interrogare innanzi tutto sulla loro ammissibilità, piuttosto che sulla loro utilizzabilità». Afferma, quindi, la Corte che i mezzi di ricerca della prova "acquisiti in violazione dell'art. 14 Cost. devono considerarsi inammissibili. Infatti l'art. 189 c.p.p., in coerenza con l'art. 190, comma 1, c.p.p. - che impone al giudice di escludere le prove "vietate dalla legge" - , presuppone logicamente la formazione lecita della prova e soltanto in questo caso la rende ammissibile. Il presupposto è implicito, dato che per il legislatore non poteva che essere lecita un'attività probatoria "non disciplinata dalla legge". È vero che con l'espressione "prova non disciplinata dalla legge" il codice si riferisce immediatamente alla mancanza di una disciplina che concerna sotto l'aspetto processuale la prova da assumere, ma è anche vero che non può considerarsi "non disciplinata dalla legge" la prova basata su un'attività che la legge vieta».

Orbene seguendo le indicazioni ermeneutiche della Corte, sembra doversi affermare che l'art. 189 consente, a certe condizioni, l'ingresso nel processo di prove non disciplinate dalla legge non rende ammissibile - in difetto di un'esplicita disposizione di legge - ogni attività posta in essere a fini investigativi e probatori dalla polizia giudiziaria e dall'autorità giudiziaria, ma solo le attività lecite e quindi non costituenti reato.

Nel caso in esame appare pacifico che l'art. 615-bis c.p. vieta, e sanziona

penalmente, l'intrusione in sistemi informatici e telematici.

Invero, come ha chiarito la Corte di Cassazione¹⁴, le condotte tipiche punite dall'art. 615-ter c.p. consistono: a) nell'introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, da intendersi come accesso alla conoscenza dei dati o informazioni contenuti nel sistema, effettuato sia da lontano (attività tipica dell'*hacker*) sia da vicino (da persona, cioè che si trova a diretto contatto dell'elaboratore); b) nel mantenersi nel sistema contro la volontà di chi ha il diritto di esclusione. Ciò che rileva, pertanto, ai fini dell'integrazione del delitto è la circostanza che l'accesso sia abusivo cioè che l'introduzione in un sistema informatico avvenga contro la volontà del soggetto che ha il diritto di esclusione, ovvero si mantiene all'interno del medesimo contro lo stesso consenso del dominus.

Non pare di alcun pregio, allora, la considerazione secondo cui l'accesso non sarebbe abusivo in quanto legittimato da un provvedimento dell'Autorità Giudiziaria alla sola condizione che dal provvedimento emerga la sussistenza di ragioni investigative. In tal modo infatti si finirebbe per rendere legittima, attraverso la disposizione dell'art. 189 c.p.p., ogni attività di regola vietata dalla legge al solo ricorrere di esigenze investigative. Questo come se la sussistenza di esigenze investigative fosse idonea a giustificare qualsiasi compressione dei diritti riconosciuti dall'ordinamento giuridico, affermazione evidentemente non condivisibile in quanto "nel nostro sistema giuridico il fine non giustifica i mezzi"¹⁵.

Il delitto citato, pertanto, sembra costituire un ostacolo insormontabile per considerare ammissibile l'utilizzo dei programmi spia al fine di captare il contenuto di un dispositivo informatico, in quanto non si è in presenza di un'area non disciplinata dalla legge - ciò che solo permetterebbe l'applicazione dell'art. 189 c.p. - ma di condotte considerate esplicitamente dall'ordinamento e dallo stesso codice penale non solo vietate, ma anche sanzionate penalmente.

6. In apertura di queste pagine si richiamava la circostanza che il mezzo di ricerca della prova in esame è costituito dall'utilizzo di "programmi spia" denominati solitamente "*trojan*" che, introdotti da remoto o *in loco*, all'interno di un sistema informatico permettono la captazione di tutta una serie di comunicazioni e dati.

Siffatta captazione può svolgersi, come è oramai chiaro, attraverso una

¹⁴ Vedi Cass., Sez. un., 27 ottobre 2011, Cassani, in *Mass. Uff.*, n. 251269.

¹⁵ Vedi in tal senso Cass., Sez. V, 13 febbraio 2009, Spada, in *Mass. Uff.*, n. 243611.

molteplicità di attività sottoposte a diversa disciplina a seconda delle loro caratteristiche.

Infatti i “programmi spia” permettono l’attivazione di una diversificata pluralità di moduli o funzioni.

Alcuni di questi rientrano nell’attività disciplinata dal codice di rito negli artt. 266 e seguenti; pacificamente sono ricomprese, in questa prima categoria, l’attivazione del microfono e/o della *web cam*, se presente sul sistema informatico, in quanto attività del tutto equiparabili all’ascolto ambientale o alle videoriprese.

Analogamente alle funzioni appena indicate l’uso di “programmi spia” per captare il flusso telematico di dati (c.d. *online surveillance*) è, anch’esso, previsto dal codice di rito dall’art. 266-*bis* c.p.p. e per il suo corretto utilizzo è, pertanto, richiesta l’applicazione della disciplina ivi prevista con il necessario intervento del G.I.P.

In ultimo. L’utilizzo di “programmi spia” per captare il contenuto, passato presente e futuro, di un sistema informatico (c.d. *online search o one time copy*) sembra essere allo stato non ammissibile nel nostro ordinamento; resta auspicabile, pertanto, al fine di non privare l’attività investigativa di un così prezioso strumento investigativo, un intervento de iure condendo, che possa disciplinare tale attività d’indagine.