LUCA MONTEVERDE

Le nuove "frontiere" delle intercettazioni

1. In un ordinamento, quello italiano, basato sull'attuazione dei principi del giusto processo, è necessario, nella costante opera di bilanciamento degli interessi in gioco, considerare sempre e comunque le garanzie e gli *standards* minimi che lo stesso processo riconosce al singolo individuo.
Se tale assunto è valido in termini generali, a maggior ragione bisogna avere massima attenzione nella fase delle indagini preliminari ed in particolar modo quando queste vertano, come nella maggioranza dei casi negli ultimi anni, su innovativi metodi investigativi riconducibili, per molte caratteristiche, alle intercettazioni in senso lato.
Il tema in questione, d'altronde, è particolarmente dibattuto e complicato data l'enorme incidenza sulla materia dello sviluppo tecnologico, che non consente di avere un quadro chiaro e ben definito: si discute, difatti, con riguardo alla possibile inclusione o meno, nella nozione di "intercettazione", di aspetti e fattispecie prima ignorati o addirittura sconosciuti, quali nuove apparecchiature GPS, "*trojan* di stato" e "appostamento informatico" che per natura e sviluppo presentano rilevanti analogie con il concetto di intercettazione stessa.
Ecco allora la necessaria focalizzazione sulle nuove "frontiere" delle intercettazioni: ci si muove in un campo sostanzialmente inesplorato ed *in itinere*.
Il rischio è che la ricerca costante di materiale probatorio, giustificata oggi dal dilagante utilizzo di moderne tecnologie per il compimento di fattispecie delittuose, possa rivelarsi fin troppo invasiva andando a ledere irreparabilmente la libertà e la *privacy* del cittadino.
Si ritiene infatti che le cautele, proprio perché ci si trova nella fase preliminare del processo, debbano essere massime poiché in presenza del principio supremo della presunzione d'innocenza.

2. Il "GPS *tracker*" è uno strumento oramai largamente utilizzato all'interno dei metodi d'investigazione in mano ai nostri inquirenti; è stato concepito dal Ministero della difesa degli Stati Uniti al fine di monitorare e tracciare gli spostamenti di persone o di oggetti sfruttando i segnali della rete satellitare GPS (*global positioning system*) e dei *chip* elettronici integrati, molto sofisticati, che dirigono l'inoltro in remoto (tramite rete GSM/GPRS della telefonia mobile) dei dati satellitari ricevuti e relativi al posizionamento del *target* anche quando i segnali sono molto deboli.

Si può subito percepire la grande potenzialità investigativa di tale strumento che, con la sua evoluzione e l'abbattimento dei costi di utilizzo, oggi è facilmente istallabile su portatili, navigatori satellitari e sempre più spesso su *smartphone* di nuova generazione, ampliando le svariate modalità d'impiego di tale sistema, dalla navigazione satellitare al monitoraggio a fini investigativi. Il tutto, utilizzando in molti casi apparecchi di proprietà dell'indagato.
La Suprema Corte ha assunto, in materia, un orientamento molto restrittivo: in tutte le sue pronunce ha rigettato le comparazioni, prospettate con vigore dalle difese, con l'istituto delle intercettazioni, facendo rientrare il monitoraggio tramite GPS in una sorta di "pedinamento elettronico".
Recentemente la Corte ha ribadito tale fattispecie offrendo molti temi d'approfondimento[1].
I Giudici di legittimità, nel caso concreto, hanno confermato l'insussistenza della prospettata illegittimità della misura della custodia cautelare basata sul c.d. *tracking devices* (controllo continuo degli spostamenti dell'indagato tramite segnale GPS proveniente dal suo cellulare), disponendo che tale attività di localizzazione del soggetto non rientri nei parametri delle intercettazioni di comunicazioni e conversazioni, bensì in una situazione di pedinamento e quindi non necessita alcuna autorizzazione da parte dell'Autorità procedente; sul punto la Corte ha affermato che «la localizzazione mediante il sistema di rilevamento satellitare (c.d. GPS) degli spostamenti di una persona nei cui confronti siano in corso indagini, costituisce una forma di pedinamento non assimilabile all'attività di intercettazione di conversazioni o comunicazioni, per la quale non è necessaria alcuna autorizzazione preventiva da parte del giudice, dovendosi escludere l'applicabilità delle disposizioni di cui agli artt. 266 e ss., c.p.p.».
Si va a ricomprendere tale monitoraggio, quindi, nell'ambito delle attività investigative c.d. "atipiche" riconducibili all'art. 189 c.p.p.; la decisione provoca, comunque, numerosi aspetti critici, in maniera particolare per la mancanza di una regolamentazione attenta e precisa che si pone così in contrasto con la tutela dei diritti costituzionalmente garantiti.
Tale decisione va a delineare un rafforzamento di un orientamento già consolidato in giurisprudenza[2]. Nel corso degli anni vi è stata un'evoluzione delle

---

[1] Il riferimento è a Cass., Sez. V, 15.01.2010, ZB e altri, n. 9667, in Diritto Penale e Processo, 12/2010, 1464 e ss..

[2] Vedi sul punto anche: Cass., Sez. V, 27 febbraio 2002, B.L. E altri, n. 16130, in *Mass. Uff.*, n. 221918; Id., Sez. IV, 1 marzo 2007, Navarro Mongort, in *Mass. Uff.,* n. 236112: «costituisce una modalità, tecnologicamente caratterizzata, di "pedinamento" e, come tale, rientra nei mezzi di ricerca della prova cosiddetti atipici o innominati attribuiti alla competenza della polizia giudiziaria (cfr. artt. 55, 347, 370 c.p.p.). Pertanto, non solo non necessita dell'osservanza delle disposizioni di cui all'art. 266 e segg. c.p.p., relative alle intercettazioni di conversazioni e/o comunicazioni, ma, non trovando comunque

metodologie investigative in materia: dall'istallazione di ricevitori GPS all'interno delle autovetture dell'indagato ad opera della polizia giudiziaria, si è passati oggi, all'utilizzo sempre più costante della tecnica del c.d. *positioning* che consiste nel tracciamento della posizione dell'individuo tramite lo *smartphone* in possesso di quest'ultimo.

La differenza sostanziale tra intercettazione e pedinamento è normalmente determinata nello scambio o meno di una qualsiasi forma di comunicazione. Si ritiene, in tal maniera, che nella situazione di *tracking* satellitare verrebbe a mancare uno dei tre presupposti che delineano l'istituto delle intercettazioni, ovvero l'apprensione di qualsiasi dato relativo ad una comunicazione. L'indagine andrebbe ulteriormente approfondita, analizzando se effettivamente l'invio di messaggi passivi, derivanti da cellulare, contenenti specifiche posizioni geografiche non possano essere comunque interpretate all'interno della nozione di "comunicazione di dati", rientranti, quindi, in un'ipotetica intercettazione telematica. Ulteriori dubbi sorgono sul rispetto dell'altrui sfera privata, nell'ipotesi in cui vengano apportate delle modiche al cellulare dell'individuo prima delle operazioni di monitoraggio, laddove possa essere istallato nel suo interno un *software* in grado di fornire all'esterno la posizione geografica[3].

La giurisprudenza, però, è pacifica nel ritenere che la comunicazione presupponga uno scambio di dati, di informazioni o di messaggi, che avviene tra due o più soggetti. Le parti essenziali della stessa sono quindi il mittente ed un ricevente: dunque una conversazione necessita sempre di due terminali attivi.

Il punto fondamentale, nell'estensione di tale fattispecie all'istituto delle intercettazioni, sarebbe, quindi, in un messaggio e nella sua ricezione. Il caso pone quindi l'interrogativo se l'attività della polizia giudiziaria nella ricezione dei segnali GPS riguardanti la posizione dell'indagato, effettivamente non possa considerarsi come un comportamento attivo e di conseguenza non farlo rientrare all'interno delle situazioni passibili di autorizzazione giudiziaria.

É proprio vero, quindi, che il flusso di dati tra emittente e ricevitore GPS non integri mai una forma di captazione?

Bisogna sottolineare, nell'analisi, orientamenti parzialmente discordanti, nati all'interno del settore delle investigazioni scientifiche e pronunciati da esperti di *digital forensis* e di ingegneria informatica.

Secondo tale impostazione la differenza, ovvero il momento in cui il monito-

---

applicazione il disposto dell'art. 15 Cost., che tutela le comunicazioni interpersonali, nemmeno appare necessario il decreto motivato del pubblico ministero, viceversa indispensabile, ad esempio, per l'acquisizione dei "tabulati" concernenti il traffico telefonico». Cass. Sez. IV, 21 gennaio 2008, B.M., in *Mass. Uff.*, n. 238679.

[3] NAZZARO, *Le intercettazioni sulle reti*, Mattioli 1885, Fidenza, 2010, 4 e ss.

raggio mediante GPS oltrepassa i confini del pedinamento elettronico entrando nel campo delle intercettazioni, sarebbe riscontrabile nella titolarità del ricevitore GPS. Nella situazione di pedinamento "*standard*" effettuata tramite, ad esempio, l'apposizione di apparecchiatura GPS di proprietà della polizia giudiziaria nella macchina del soggetto destinatario dell'atto, il flusso di comunicazioni sarebbe inerente la polizia giudiziaria, senza andare a ledere la *privacy* del soggetto. Viceversa, qualora il flusso si acquisisca tramite i dati di un rilevatore GPS di proprietà del soggetto destinatario dell'atto, tale attività potrebbe essere interpretata come una vera e propria intercettazione digitale avente ad oggetto un flusso il cui titolare, appunto, è il soggetto medesimo.
Tornando all'inserimento, da parte della giurisprudenza, del pedinamento satellitare all'interno dei canoni previsti dall'art. 189 c.p.p., la collocazione sistematica della norma e l'impiego del termine "prova" lascerebbe presagire un utilizzo dello strumento riservato esclusivamente alla fase processuale, tuttavia, per idea consolidata in dottrina, il pedinamento satellitare sarebbe destinato a realizzarsi anche nella fase d'investigazione[4].
Quanto al rispetto dei parametri contenuti all'interno della norma citata, il mezzo investigativo atipico non sembrerebbe porre notevoli interrogativi. In relazione alla idoneità «ad assicurare l'accertamento dei fatti» da provare sorgono pochi dubbi, osservando l'alto livello di attendibilità dei dati GPS che rivelano la posizione del soggetto, offrendo strumenti adeguati per una ricostruzione veritiera degli accadimenti. Quanto al secondo presupposto richiesto dall'art. 189 c.p.p., ovvero la necessità che il dispositivo utilizzato non vada ad incidere sulla libertà morale del soggetto, essendo un mezzo investigativo che può predisporre un congruo risultato solamente nel caso in cui sia totalmente al di fuori della conoscenza del soggetto sottoposto a controllo, ne risulta che quest'ultimo non possa in nessun modo esservi condizionato.
Rimane, però, irrisolto il problema di fondo riguardante le modalità in cui i dati del pedinamento satellitare possono essere introdotti e utilizzati dinanzi al giudice dibattimentale.
Gli atti derivanti dalle indagini preliminari vengono trattati in maniera diversa in fase di dibattimento, a seconda che questi ultimi siano ripetibili o irripetibili, a prescindere dalla tipicità del tipo di prova che si utilizza. È noto che l'atto ripetibile possa trovare accesso in fase dibattimentale tramite esperimento realizzato davanti al giudice, le cui modalità, in caso di prova atipica, andranno stabilite in maniera preventiva e nel contraddittorio tra le parti, come previsto dall'art. 189, co. 2, c.p.p., viceversa gli atti irripetibili accedono alla scena

[4] NOBILI, *Commento al nuovo codice di procedura penale*, coordinato da Chiavario, II, Torino 1990, 387.

dibattimentale ai sensi dell'art. 431, co. 1, lett. b), c.p.p. e sono impiegabili dal giudice nella predisposizione della sua decisione finale.

L'art. 431, co. 1, lett. b), parla di verbali di atti irripetibili da ottenere, ma nel pedinamento satellitare siamo di fronte a delle rappresentazioni tramite cartografie elettroniche, poiché le elaborazioni dei dati realizzati mediante rilevazioni GPS vengono poi inserite su dei supporti magnetici. Resta da chiarire, quindi, nel conseguimento degli atti irripetibili, se vada acquisito il solo verbale di documentazione dell'attività di pedinamento elettronico, o piuttosto, anche il supporto informatico che contiene tali informazioni[5].

La vera questione nasce dal continuo orientamento giurisprudenziale che valuta come irripetibili gli atti riguardanti il pedinamento elettronico – con la conseguenza che un'attività rientrante nella libera disponibilità della p.g. – senza obbligo di autorizzazione da parte dell'Autorità giudicante, compiuta nelle indagini preliminari e senza le garanzie difensive che sono previste per gli accertamenti tecnici irripetibili, arrivi nella fase processuale senza alcun tipo di filtro e di controllo[6].

Da una comparazione di tale approccio giurisprudenziale con il dettato costituzionale, e nel dettaglio con i diritti inviolabili contenuti nella prima parte della nostra legge fondamentale, si possono ricavare ulteriori temi di dibattito.

A tal fine bisogna mettere in relazione il combinato disposto dagli artt. 13, 14, 15 Cost. con l'art. 112 Cost., la cui predisposizione può portare, ad avviso della Consulta, ad una "compressione" delle altre libertà garantite dalla prima parte della Costituzione, sempre nel rispetto dei diritti fondamentali dell'individuo.

È necessario considerare tale metodo di pedinamento in relazione al diritto di riservatezza, contenuto all'interno dell'art. 15 Cost.

L'orientamento giurisprudenziale non facendo rientrare tale attività investigativa all'interno dell'istituto dell'intercettazione, non ravvede, quindi, nessuna lesione del principio di segretezza delle comunicazioni, poiché in questa fattispecie non c'è alcuna conversazione che viene captata.

Occorre, a parere di chi scrive, effettuare un'analisi più profonda di tale situazione: l'intrusione nell'altrui sfera privata si esaurisce davvero nella sola captazione di una comunicazione?

Con l'incessante sviluppo tecnologico, è cresciuta anche la necessità di salvaguardia per i cittadini de c.d. "dati sensibili"; il monitoraggio elettronico via GPS con certezza provoca un'intrusione molto più profonda nella sfera priva-

---

[5] Autorevole dottrina sostiene che vada appreso sia il verbale documentativo delle operazioni sia il supporto informatico. Sul punto: CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove incostituzionali*, in *Cass, pen.,* 1999, 1192 e ss.

[6] VELANI, *Nuove tecnologie*, in *Giur. it.*, 2003, 2373.

ta del singolo, soprattutto per la minuziosità dell'indagine e per la possibilità di protrarla per lunghi periodi[7]. Non è solo la libertà di comunicazione a dover essere garantita e protetta, ma il legislatore dovrebbe tener conto di quelle che sono a tutti gli effetti le "nuove" libertà derivanti dal processo tecnico-scientifico, che danno la possibilità di nuove violazioni della vita privata[8].

3. Metodologia perfino più invasiva è sicuramente data dal recentissimo impiego da parte degli investigatori del c.d. "captatore informatico".
L'acquisizione occulta *on-line* e da remoto dei contenuti digitali di un supporto informatico collegato alla rete Internet è una di queste nuove tecniche d'investigazione utilizzate oggi anche dalle forze di polizia per introdursi negli spazi informatici dove vi è motivo di ritenere possano nascondersi delle attività criminose.
Ma si può ritenere totalmente in linea con i principi del giusto processo tale attività?
La Suprema Corte si è pronunciata sull'argomento nella sentenza n°16556 del 29 aprile 2010.
Il fatto ha origine dall'impiego dei risultati dell'attività di indagine disposta dal Pubblico ministero con decreto del 22 aprile 2004.
Il decreto di acquisizione di atti, ai sensi dell'art. 234 c.p.p., aveva ad oggetto l'acquisizione in copia, tramite un *malware*, della documentazione informatica memorizzata all'interno del *personal computer* utilizzato da uno degli imputati e localizzato presso alcuni uffici Comunali.
Le eccezioni difensive si basarono sul fatto che il provvedimento del p.m., pur autorizzando una mera acquisizione in copia di atti, potesse essere ricompreso all'interno dell'istituto delle intercettazioni telematiche *ex* art. 266-*bis* c.p.p., e che quindi difettasse dell'assenza del provvedimento autorizzativo da parte dell'Autorità.
Invero, il decreto avrebbe disposto non solo l'acquisizione di quei *files* che erano stati già composti dall'utente, ma anche di tutti quei documenti che sarebbero stati realizzati in futuro, in modo da memorizzarli nel lungo periodo.
Le concrete modalità di investigazione consistettero nell'istallazione nel *personal computer* dell'indagato di un virus denominato "*trojan horse*", che dà la possibilità a colui che lo utilizza di prendere totalmente in controllo il dispositivo sul quale è installato.
Tutte le eccezioni difensive, in materia, furono rigettate dalla Suprema Corte.

---

[7] LYON, *La società sorvegliata: tecnologie di controllo della vita quotidiana*, Philadelphia , 2001, 46-52.
[8] GENTILE, Tracking *satellitare mediante gps: attività atipica di indagine o intercettazione di dati?,* in *Dir. pen. proc.*, 2010, 1464 e ss.

Si sottolineò come il decreto del pubblico ministero si limitava a disporre delle operazioni di estrazione di dati, sia di quelli già contenuti all'interno della memoria del *personal computer* dell'indagato, sia di quelli che sarebbero stati formati in futuro. Chiarì inoltre la definizione di flussi di comunicazioni riprendendo una sentenza passata della stessa Corte di legittimità: «per flusso di comunicazioni deve intendersi la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un ricevente, da un soggetto ad altro, ossia il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici»[9]. Non interpretò, quindi, tale situazione passibile di intercettazione poiché consisteva in captazione di «una elaborazione del pensiero e la sua esternazione in scrittura su di un *personal computer* oppure mediante simboli grafici apposti su un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura ed in tal modo memorizzato».

Nel particolare l'attività di autorizzazione del pubblico ministero consisteva nel prendere e copiare, non solo i documenti presenti, ma anche quelli che si sarebbero formati all'interno del computer dell'indagato, che era posizionato in un ufficio comunale. Secondo l'accusa, quindi, non si trattava di una captazione di un «flusso di comunicazioni», che richiede un dialogo con altri soggetti, ma di «una relazione operativa tra microprocessore e video del sistema elettronico ossia un flusso unidirezionale di dati confinato all'interno dei circuiti del *personal computer*».

Per questi motivi, i risultati di tale provvedimento erano legittimi, poiché interpretabili ai sensi dell'art. 189 c.p.p., catalogando tale attività come "prova atipica".

La Corte ha replicato ritenendo che l'attività captativa non avesse violato né l'art. 14 Cost., né l'art. 15 Cost. Secondo i Supremi Giudici: «il computer monitorato con l'installazione del captatore informatico non era posto in un luogo domiciliare o in un luogo di privata dimora, bensì in un luogo aperto al pubblico. Il *personal computer*, pertanto, si trovava nella locale sede di un ufficio pubblico comunale, dove sia l'imputato sia gli altri lavoratori accedevano per disporre le loro mansioni e dove potevano fare ingresso il pubblico degli utenti e il personale addetto alle pulizie dello stabile, quindi una comunità di persone non particolarmente ampia, ma nemmeno limitata o determinabile *a priori* in ragione di una determinazione personale dell'imputato».

D'altro canto, nel caso concreto, non si poteva invocare la tutela costituziona-

---

[9] ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del* cloud criminal, IISFA Memberbook, 2013, Forlì 1-13.

le della riservatezza della corrispondenza e in genere delle comunicazioni, poiché quanto duplicato in copia non era un testo inoltrato e spedito tramite un sistema informatico privato e personale, ma «soltanto predisposto per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario».

La Corte ha richiamato, inoltre, le conclusioni della Corte d'Appello che aveva respinto l'attuazione della disciplina degli accertamenti tecnici irripetibili, poiché «l'attività di riproduzione dei *files* memorizzati non aveva comportato l'alterazione, né la distruzione dell'archivio informatico, rimasto immutato, quindi consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria. Si era trattato di un'attività sempre reiterabile, alla cui esecuzione non era necessaria la partecipazione del difensore, poiché la stessa poteva essere compiuta una seconda volta se solo si fosse poi approdato ad uno sviluppo dibattimentale del procedimento».

In conclusione, con tale sentenza, la Corte ha ritenuto legittimo l'atto del pubblico ministero, nella misura in cui il provvedimento ha riguardato la memorizzazione di dati non aventi ad oggetto un flusso di comunicazioni già formati e contenuti nella memoria del "*personal computer*", qualificando tale attività di acquisizione di documenti come prova atipica e sottraendola alla disciplina prescritta dagli artt. 266 ss., c.p.p.

Nel caso concreto appare corretta l'impostazione della Corte nel non ritenere l'attività di apprensione dei *files word* composti dall'imputato come una vera intercettazione *ex* art. 266 e ss., proprio perché manca il soggetto al quale tali comunicazioni erano rivolte e quindi mancano i due terminali attivi di un comportamento comunicativo: mittente e destinatario.

Quello che non è dato sapere è se l'attività di captazione si sia effettivamente limitata a questo; se il computer in questione era connesso ad internet e in tal caso se fossero stati acquisiti anche dati di comunicazioni VoIP[10] o comunicazioni effettuate su *chat* e piattaforme simili.

Dalla sentenza non emerge affatto questa situazione, pertanto si deve ritenere che il PC non venisse impiegato facendo uso di queste forme di comunicazione tra soggetti diversi.

Un punto molto interessante è rinvenibile nelle caratteristiche di questo programma utilizzato per la captazione, caratteristiche che non sono note e con alta probabilità non sono state neanche riportate nei verbali della polizia giudiziaria, facendo venire meno garanzie e controllo sulle operazioni predisposte con un *software* altamente tecnologico.

Stupisce anche la decisone della Corte di cassazione nella parte in cui ritiene

[10] Chiamate che utilizzano la rete Internet: *Voice over Internet Protocol*.

che la prova raggiunta sia una prova atipica e quindi disciplinata dall'art. 189 c.p.p.
Nella fattispecie, a ben vedere, trattandosi di *files* informatici contenuti su supporti informatici tipizzati e inseriti nel nostro ordinamento con la l. 23 dicembre 1993, n. 547, non è tanto in discussione la prova atipica ma il mezzo con la quale è stata raggiunta: ovvero l'utilizzo di mezzi di ricerca della prova atipici.
Si dibatte, in dottrina, se possa davvero esistere tale categoria, soprattutto se le circostanze del caso in questione permettano agli inquirenti la "ricerca della prova" utilizzando situazioni di indagine più diffuse: sequestro, ispezioni.
Alcuni, quindi, negano la possibilità di utilizzo di tali mezzi non previsti dal codice di rito, sottolineando che i mezzi di ricerca della prova sono utilizzati il più delle volte, nel corso delle indagini preliminari, in situazioni nelle quali è impossibile il contraddittorio con la difesa davanti al giudice come indica l'art. 189 c.p.p.[11].
Al contrario la tesi maggioritaria, e le Sezioni unite della Suprema Corte[12], hanno delineato la possibilità di svolgimento di tali fattispecie atipiche, come ad esempio le video-riprese d'immagini in spazi differenti dal domicilio, attraverso un'interpretazione estensiva dell'art. 189 c.p.p. (nel senso di predisporre un contraddittorio posteriore e successivo sugli elementi acquisiti con tali mezzi). Solo seguendo questa impostazione sembrerebbe rispettato il principio di legalità.
Nel caso concreto, appare di tutta evidenza, come tale impostazione possa essere accolta proprio perché il computer dell'indagato non era posizionato all'interno del proprio domicilio.
Laddove il computer in questione fosse stato all'interno della privata dimora dell'indagato sicuramente non sarebbe stato compito facile, per la Suprema Corte, giungere alle medesime conclusioni.
Le conclusioni della Corte, inoltre, non appaiono condivisibili quando si afferma che «nella specie, dovesse essere osservata la disciplina prevista per gli accertamenti tecnici irripetibili, atteso che l'attività di riproduzione dei *files* memorizzati non aveva comportato l'alterazione, né la distruzione dell'archivio informatico, rimasto immutato, quindi consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria. Si era trattato di un'attività sempre reiterabile, alla cui esecuzione non era necessaria la partecipazione del difensore, poiché la stessa avrebbe potuto essere compiuta una seconda volta se si fosse approdato ad uno sviluppo di-

[11] TONINI, *Manuale di procedura penale*, Milano, 2013, 258.
[12] Cass., Sez. un., 28 marzo 2006, Prisco, in *Riv. pen.,* 2007, 459.

battimentale del procedimento».
Le eccezioni della difesa si sono concentrate su questo punto, andando a sostenere che «non era stata osservata la disciplina riguardante gli accertamenti irripetibili, con un'ulteriore violazione di legge» in relazione al mancato avviso ai difensori e alle parti, ma la Corte ha rigettato anche questo punto.
Ulteriormente la Corte non sottolinea né motiva il fatto che un sistema nel quale viene installato un "*trojan horse*" viene comunque alterato a livello strutturale; con il captatore all'interno si vanno a mutare alcune funzioni di sistema specifiche che danno la possibilità al tecnico collegato da remoto, e connesso alla rete, di prendere il possesso dell'apparecchiatura e di far eseguire allo strumento stesso una serie di operazioni che sono fuori dal controllo dell'utente autorizzato, andando a modificare evidentemente altre funzioni tipiche di sicurezza del sistema proprio per permettere l'installazione del *virus*. Anche in maniera accidentale i contenuti di un sistema informatico possono essere alterati da tale "*malware*" e quindi la difesa non potrebbe essere in grado di andare a ripetere le operazioni di acquisizione dei dati ottenendo lo stesso risultato della polizia giudiziaria, ovvero non ottenere lo stesso contenuto dell'*hard disk* in quanto è mutato per l'installazione nel *software* del "*trojan*".
È molto discutibile, pertanto, la tesi su questo punto, proprio perché non si può esprimere con certezza che l'attività sia sempre reiterabile. Non può essere, difatti, garantita l'effettiva integrità e genuinità dei *files* ottenuti e quindi una prova modificata unilateralmente non sembra, in nessun modo, concepibile all'interno dei principi del giusto processo delineati dall'art. 111 della nostra Costituzione.
Sul punto, si può dire inoltre, che esistono ed esistevano anche ai tempi del provvedimento autorizzativo del 2004, tecniche di garanzia riguardo l'immodificabilità dei *files* captati da remoto, il c.d. *hashing,* che avrebbero potuto garantire l'integrità e la genuinità dei *files* captati se effettuate prima dell'operazione e soprattutto con criterio e con la finalità di far verificare alla difesa la genuinità della prova.
Più in generale si dà il merito a tale sentenza di aver comunque portato alla luce un problema molto importante, che dovrebbe essere risolto il prima possibile a livello legislativo, ovvero una regolamentazione sull'ammissibilità giuridica di tali captatori che, inoltre, con il passare degli anni diventano sempre più tecnologici e con capacità di intrusione sempre maggiore e più penetrante nella sfera privata del singolo[13].

[13] ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del* cloud criminal, cit., 9 e ss.

Il problema è molto serio, anche perché si conoscono a malapena le grandissime potenzialità di tali strumenti che sono in costante sviluppo; tali *virus* ad oggi hanno la capacità di prendere totalmente il controllo del computer ospite, acquisire e memorizzare tutti i *files* presenti nel *software* ed inviarli direttamente all'operante; accendere e spegnere microfono e *web-cam* eventualmente presenti; ed infine dare la facoltà di *uplodare files* e documenti salvandoli nel sistema.
Valutando la grande invasività dello strumento sorgono spontanee alcune domande: quali sono le garanzie del pubblico ministero che emette il decreto e autorizza le captazioni? Qual è l'effettivo controllo della polizia giudiziaria su quelle che sono le attività del tecnico che svolge le operazioni sul pc "*target*"?
A queste domande non è possibile rispondere poiché la procedura non è disciplinata ma lasciata alla discrezionalità delle diverse squadre di polizia giudiziaria e dei pubblici ministeri.
Si potrebbe, ad esempio, richiedere la redazione di un verbale da parte della polizia giudiziaria, con elenco dettagliato delle operazioni che vengono eseguite, l'indicazione delle specifiche caratteristiche del "*malware*" (in questo senso la difesa deve sapere cosa è in grado di fare il *software* utilizzato), di date o orari nonché relazione del monitoraggio effettuato, questi semplici passaggi renderebbero certamente l'impiego di tali dispositivi più in linea con i principi del giusto processo richiamati sia dalla nostra Costituzione, sia sottolineati dall'art. 6 C.e.d.u.
Considerando, inoltre, la delicatezza e l'intrusività delle azioni operative che si realizzano mediante tali strumenti sarebbe desiderabile una contemporanea attività d'intercettazione telematica di quelli che sono i flussi informatici derivanti dal PC "intercettante", e quindi dell'utente collegato al computer della polizia giudiziaria o del consulente tecnico, al fine di monitorare, controllare e preservare l'indagato da eventuali *upload* di nuovi programmi o documenti anche involontari.
Il problema di fondo è che in uno stato di diritto improntato su principi di legalità e con garanzie processuali codificate, la corsa al risultato ad ogni costo non può e non deve competere e sopravanzare le garanzie processuali, le esigenze difensive ed il controllo del giudice delle indagini preliminari con riferimento alle modalità investigative che mettono in pericolo i diritti inviolabili del cittadino.

4. In continuo aumento sono, poi, i casi nei quali i giudici si trovano a che fare con reati derivanti dall'utilizzo illegale del mondo di internet e soprattutto dall'impiego distorto di pagine *web.*

Queste situazioni creano notevoli problemi a coloro che devono giudicare, ma soprattutto a coloro che devono investigare su tali tipi di reato. Le principali difficoltà nella ricostruzione dei reati c.d. "globalizzati" riguardano difatti la dislocazione dell'autore, l'indeterminatezza degli autori, anonimizzazione, cronologia degli eventi e modalità esecutive della fattispecie delittuosa[14].

La totalità della disciplina merita di essere approfondita in corrispondenza della specificità dell'oggetto d'accertamento, costituito da quelle situazioni informatiche che formano l'impianto probatorio di ogni processo riguardante un *computer crime*. Non vi sono dubbi, difatti, che in relazione alla facile modificabilità e volatilità delle stesse il sistema normativo si sia modellato anche grazie alle elaborazioni dottrinali in materia che affermano come «il giusto processo deve riconoscere all'imputato il diritto di essere messo a confronto con il dato informatico nella sua genuinità, senza alterazioni», ponendo in evidenza, come «questa sia la trasposizione moderna del diritto a confrontarsi con l'accusatore»[15].

In materia si deve analizzare sicuramente lo svolgimento di attività di "appostamento informatico" – utilizzato da parte della polizia giudiziaria per tracciare elementi riguardanti fattispecie di reato commesso tramite sistemi informatici – analizzato, verosimilmente per la prima volta in Italia, all'interno del caso *svanityfair.com*.

Il caso[16] riguardava la pubblicazione di numerosi articoli diffamatori, secondo la Procura, su tale sito: gli inquirenti ricercarono, tramite un preliminare tracciamento del sito e delle *mail* collegate a quest'ultimo, chi fosse l'effettivo gestore.

All'interno della sentenza vengono ben delineate quelle che furono le attività degli investigatori che sfruttarono l'invio di c.d. "*e-mail* civetta" contenti un codice *"html"* per tracciare l'indirizzo IP del soggetto, desumere la tipologia del *browser* utilizzato ed acquisire implicitamente dalle comunicazioni con l'indagato ogni informazione utile alla vicenda.

Siamo di fronte ad una vera ed occulta introduzione, da parte della p.g., in uno dei due terminali attivi della conversazione al fine di intercettare dati inerenti l'ipotesi di reato in questione.

Il pubblico ministero, però, chiarì nella requisitoria svolta il 28 ottobre 2009, come fosse stata del tutto corretta l'attività della polizia giudiziaria, su specifica delega di quest'ultimo, nell'inviare delle *mail* alle quali l'indagato aveva "abboccato", perché, proprio per aver risposto a tali *mail*, aveva «implicitamente

---

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

[16] Tribunale di Milano, Sez. VII, 15 marzo 2010, D.G., n. 1877.

comunicato una serie di dati tecnici, i quali adeguatamente elaborati e sviluppati, anche con la collaborazione del gestore della telefonia, avevano condotto alla sua compiuta e precisa identificazione».
Il rappresentante della pubblica accusa non riteneva, innanzitutto, si fosse di fronte alla figura del c.d. "agente provocatore" poiché non vi era stata nessuna induzione alla commissione di reati, ma, in maniera assai discutibile, non riteneva vi fosse necessità di alcuna preventiva autorizzazione allo svolgimento di tale attività.
Lascia molti dubbi il fatto che non sia stata considerata come intercettazione tale fattispecie: in questo caso vi sono due terminali attivi, un mittente – la polizia giudiziaria con le *e-mail* "traccianti" – e un destinatario partecipe, appunto l'indagato. In questo frangente si ha a che fare con un comportamento comunicativo vero e proprio, anche se non telefonico e quindi vocale: le risposte che hanno «implicitamente comunicato una serie di dati tecnici» denotano chiaramente, quindi, l'attività oggettiva di captazione di tali informazioni da parte della polizia giudiziaria, che in quanto tale dovrebbe essere autorizzata dall'Autorità competente.
Ma la motivazione del giudice è di tutt'altro avviso: si legge che «trattasi quindi di mezzo di ricerca della prova atipico, pacificamente ammissibile secondo i principi del nostro codice di procedura penale. [...] L'inquadramento di tale mezzo di indagine nella categoria dei mezzi di ricerca della prova cosiddetti atipici o innominati pone, in primo luogo, la questione circa le condizioni di ammissibilità delle prove non disciplinate dalla legge, alle quali fa riferimento l'art. 189 del codice di procedura penale. Secondo le previsioni di tale norma, quando è richiesta una prova atipica, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e se non pregiudica la libertà morale della persona; si provvede poi alla sua ammissione solo dopo aver sentito le parti sulle modalità di assunzione della prova».
Dunque, per l'ammissibilità della prova atipica, la norma pone due condizioni di carattere sostanziale: la sua idoneità ad assicurare l'accertamento dei fatti e la mancanza di pregiudizio per la libertà morale della persona; inoltre, è posta anche la regola procedurale secondo cui va assicurato il contraddittorio delle parti sulle modalità di assunzione della prova.
Il citato disposto normativo, secondo la prevalente ricostruzione dottrinaria, ha la sua *ratio* nell'esigenza di adeguare il sistema probatorio all'evoluzione del progresso scientifico e tecnologico.
È altresì nota l'impostazione, comunemente condivisa dagli studiosi, secondo cui, pur essendo tale disposizione collocata nel libro III del c.p.p. dedicato alle prove, essa è applicabile all'intero arco del procedimento, anche in via analogica e, dunque, anche nella fase delle indagini preliminari. In particola-

re, secondo il richiamato orientamento, è l'intero titolo I dedicato alle disposizioni generali, che sarebbe applicabile alla fase investigativa.
Ma si può davvero interpretare tale situazione come mezzo di indagine atipico? Non si lascia troppo spazio di azione nelle mani degli inquirenti? Sono rispettate le norme riguardanti il *fair play* processuale e le parità d'armi tra accusa e difesa?
Nella sentenza d'appello[17]sono state confermate le tesi del giudice di primo grado, disponendo che tale attività non rientra nell'istituto delle intercettazioni telematiche poiché riguarda «attività d'indagine assimilabile al pedinamento/appostamento a distanza a mezzo satellitare, utilizzato nella prassi investigativa per accertare tempi e luoghi di spostamento di una persona in movimento, sulla cui legittimità quale "*m*ezzo di ricerca di prova atipica e innominata" regolata dall'art. 189 si è più volte espressa la Suprema Corte». Per la Corte d'appello «l'appellante sembra ignorare i passaggi essenziali della motivazione ed in particolare la considerazione che le intercettazioni regolate dagli artt. 266 e 266-*bis* c.p.p. attengono ad attività di ascolto e registrazione di comunicazioni tra due o più persone», andando nuovamente a comparare tale attività, in maniera abbastanza discutibile proprio perché in questo caso si delineano e si captano dei contenuti comunicativi nelle *mail*, con quella del pedinamento satellitare tramite GPS, fornendo un'interpretazione del concetto di comunicazione quantomeno restrittiva e non in linea con quelle che sono le esigenze della tecnologia di oggi.

5. È auspicabile, pertanto, un repentino intervento del legislatore in materia volto a spiegare effettivamente perché questi mezzi di ricerca della prova "atipici" non integrano una intercettazione telematica, andando a mutare, laddove ce ne sia il bisogno, anche il concetto di "comunicazione". Si denota, infatti, l'esigenza di porre dei limiti a questi strumenti, data la loro invasività nei confronti di diritti che non possono essere lasciati in secondo piano, e si auspicano norme che richiamino principi di chiarezza e trasparenza al fine di garantire il rispetto del principio di parità tra difesa e accusa che, in questa materia, appare quantomeno messo in discussione. In conclusione, si dovrebbe tener conto anche di quelli che sono i "nuovi" diritti e le "nuove" libertà che stanno nascendo nella nostra società.
Non può negarsi che, ormai, la maggior parte dei cittadini utilizzi la rete come un vero e proprio centro di "gestione" dei propri affari, che riguardino l'attività lavorativa o che rientrino nella sfera privata del soggetto; sarebbero pertanto auspicabili interventi normativi, soprattutto in relazione alla possibili-

[17] Corte d'Appello di Milano, Sez. I, 11 maggio 2012, D.G.

tà di tutelare il "domicilio informatico", al fine di limitare indagini investigative telematiche che oltrepassino le norme e i principi del codice di procedura penale, oltre che la carta costituzionale, e richiedere per tali attività che, senza dubbio sono lesive e intrusive della sfera privata del soggetto, un adeguato controllo giurisdizionale.

L'adeguamento del sistema probatorio con riguardo alla "evoluzione del processo scientifico e tecnologico" ed il parallelo sviluppo di nuove "frontiere" dell'intercettazione devono far riflettere: si richiede una maggior sensibilità da parte dei giudici, ma soprattutto da parte del legislatore nell'andare a regolamentare una materia che interessa i diritti fondamentali del cittadino. In uno Stato di diritto che voglia assumersi come "moderno", infatti, non sono accettabili lesioni del diritto di difesa e dell'equo processo in favore di un'insaziabile e ossessiva ricerca di una verità "assoluta".