2/2018

UNA PROPOSTA COSTITUZIONALMENTE ORIENTATA PER ARGINARE LO STRAPOTERE DEL CAPTATORE

Dalla sentenza Scurato alla riforma Orlando

di Mario Griffo

Abstract. *Il captatore informatico costituisce uno straordinario strumento investigativo ma anche un meccanismo in grado di incidere in maniera devastante nella vita "intima" dell'individuo "bersaglio". Da ciò lo sforzo profuso nel tentativo di contemperare le due esigenze in conflitto. Risultato: gli approdi della "riforma Orlando". Per taluni la auspicata copertura normativa all'impiego di un imprescindibile ed infallibile ausilio alla indagine penale, per altri soltanto l'abbrivio per un complessivo ripensamento in senso maggiormente garantista della materia.*

1. Cos'è il captatore informatico?

Il virus trojan prende il suo nome, verosimilmente, dal leggendario cavallo di Troia che, per mezzo di Odisseo, l'uomo dal multiforme ingegno, riuscì ad entrare dentro le mura di Troia, con inganno, ed espugnarla. Così come il cavallo di Troia sconfisse i troiani entrando all'interno della loro cittadella muraria, fingendosi un dono pregiato da parte degli Achei, così anche il predetto virus riesce ad entrare, con inganno, nell'apparecchio (attraverso una richiesta di download[1], ad esempio) che si

[1] Il download, o scaricamento, indica in informatica l'azione di ricevere o prelevare da una rete telematica (ad esempio da un sito web) un file, trasferendolo sul disco rigido del computer o su altra periferica dell'utente. Nella maggior parte dei casi lo scaricamento di un file è la conseguenza di una richiesta, più o meno trasparente all'utente del sistema. L'azione inversa è invece detta upload. Ogni volta che un computer connesso a Internet richiede una pagina o un qualsiasi contenuto su internet, un computer

vuole intercettare, non per distruggerlo né tanto meno per danneggiarlo, ma per carpire qualsiasi dato che ivi possa trovarvi. Tali programmi, per vero, sono concepiti e costruiti per istallarsi in modo occulto sui congegni elettronici che si vuole monitorare ed agiscono senza rilevare all'utente la propria presenza.

Inviando un simile virus informatico, in altri termini, è possibile installare negli smartphone, nei tablet e nei computer un software in grado di far controllare l'apparecchio da una postazione remota. L'ufficiale di polizia giudiziaria che opera tale controllo può decifrare tutto ciò che viene digitato sulla tastiera; visualizzare quel che appare sullo schermo; monitorare la navigazione in internet; perquisire i files contenuti nell'hard disk o salvati in cloud; accedere alle applicazioni di posta elettronica e di messaggeria; visualizzare i messaggi inviati e ricevuti e intercettare quelli in entrata e uscita; intercettare le conversazioni telefoniche; attivare il microfono ed effettuare intercettazioni ambientali nel raggio di una decina di metri dall'apparecchio; attivare la videocamera e riprendere quanto viene inquadrato[2].

Tutte le volte che si parla di captatore informatico in ambito investigativo, tuttavia, è necessario distinguere tra due diverse modalità operative: quella online search e quella online surveillance. I programmi appartenenti alla prima categoria consentono di fare copia, totale o parziale, delle unità di memoria del sistema informatico individuato come obiettivo. I dati sono trasmessi in tempo reale o ad intervalli prestabiliti agli organi di investigazione tramite la rete internet in modalità nascosta e protetta. Attraverso i programmi online surveillance è possibile, invece, captare il flusso informatico intercorrente tra le periferiche — video, microfono, tastiera, webcam — ed il microprocessore del dispositivo bersaglio, consentendo al centro remoto di controllo di monitorare in tempo reale tutto ciò che viene visualizzato sullo schermo c.d. screenshot[3], digitato sulla tastiera c.d. keylogger[4] o pronunciato al

---

remoto invia l'oggetto richiesto attraverso una rete di calcolatori fino al computer che aveva inviato la richiesta, il quale riceve i dati sotto forma di pacchetti da ricostruire. All'interno di questo meccanismo la richiesta di download, che pure prevede l'invio di informazioni al sistema remoto, non viene definita propriamente upload (in italiano "caricamento") in quanto vengono trasferite solo le informazioni necessarie per sincronizzare il trasferimento dei dati. Per questo motivo lo scaricamento di un file comporta necessariamente anche l'utilizzo di parte di banda dell'upload; nel caso in cui la banda in caricamento sia satura la velocità dello scaricamento si autolimiterà (voce *Download*, in *Treccani.it*, *Enciclopedie on line*, Istituto dell'Enciclopedia Italiana, 15 marzo 2011).

[2] Vedi ATERNO, Digital forensics (investigazioni informatiche), in *Dig. pen.*, Agg. VIII, Utet giuridica, 2014, p. 245, ss.; BALSAMO, *Le intercettazioni mediante virus informatico, tra processo penale e Corte Europea*, in *Cass. pen.*, 2016, p. 2274 ss.; FILIPPO, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen.*, 2016, n. 2, p. 11 ss.; IOVENE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont. – Riv. trim.*, 3-4/2014, p. 330; NOCERINO, *Le Sezioni unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale*, in *Cass. pen.*, 2016, p. 3566 ss.; TESTAGUZZA, *I sistemi di controllo remoto: tra normativa e prassi*, in *Dir. pen. proc.*, 2014, p. 759; TONINI-CONTI, *Il diritto delle prove penali*, Milano, 2014, p. 480.

[3] Il termine inglese screenshot (da screen che significa "schermo" e shot invece "scatto fotografico"), in italiano fermo-immagine, schermata o immagine dello schermo, indica ciò che viene visualizzato in un determinato istante sullo schermo di un monitor, di un televisore o di un qualunque dispositivo video. Nell'ambito dell'informatica il fermo-immagine è il risultato della cattura (istantanea) di ciò che è visualizzato sul monitor del computer. Va precisato che nella terminologia inglese lo screenshot indica solo il processo che cattura l'area dello schermo e che la memorizza nel buffer di sistema, in modo da

microfono. Si tratta di softwares che, prescindendo dalle autorizzazioni dell'utente, si installano in un sistema scelto come obiettivo e ne acquisiscono qualsiasi informazione.

2. Lo statuto del captatore nel contesto delle intercettazioni ambientali.

I captatori informatici vengono utilizzati dalle forze dell'ordine da anni. Qualche esempio: il caso di Luigi Bisignani. Infatti, nell'inchiesta sulla P4 è stato fondamentale l'uso di un programma che ha trasformato il computer del faccendiere in una microspia: nome in codice "Querela".

O, ancora, l'arresto di Rocco Schirripa accusato di essere l'omicida del procuratore Bruno Caccia, ucciso nel giugno del 1983. Anche qui, secondo quanto riportato dalle cronache, il trojan ci avrebbe messo lo zampino.

Lo stesso Giulio Occhionero afferma di essere stato incastrato dalla polizia con un malware[5].

"Un utilizzo che diventerà sempre più frequente man mano che internet verrà cifrata di default, determinando una perdita delle capacità investigative tradizionali", ha spiegato, nel 2015, a *Repubblica* Fabio Pietrosanti, cofondatore del Centro Hermes per la trasparenza e i diritti umani digitali.

Di quali siano le loro capacità si può solamente immaginarlo: potenzialmente infinite.

---

poterla trasferire (incollare) in un documento (ad esempio, un documento di Paint). Nella terminologia italiana esso indica invece anche l'operazione di memorizzazione della cattura della schermata in un file (in inglese è tecnicamente detto screen dump), l'immagine riprodotta (per esempio a mezzo stampa) o la composizione di un filmato da una sequenza di catture dello schermo, in inglese è tecnicamente detto screen capture (In argomento, DAVID THOMAS, KYLE ORLAND, SCOTT STEINBERG, *The videogame style guide and reference manual*, Power Play Publishing, 2007, p. 57, ISBN 978-1-4303-1305-2).

[4] In informatica un keylogger è uno strumento hardware o software in grado di effettuare lo sniffing della tastiera di un computer, cioè è in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente si accorga di essere monitorato. Il classico keylogger hardware consiste in un dispositivo elettronico da collegare sul cavo di comunicazione tra la tastiera ed il computer o è posizionato direttamente all'interno della tastiera stessa. Il dispositivo contiene un circuito elettronico che rileva la sequenza di segnali corrispondenti ai pulsanti utilizzati sulla tastiera e la memorizza nella memoria interna. Alcuni possono inviare i dati in rete o essere monitorati e comandati in remoto, in alternativa il dispositivo può essere recuperato fisicamente o i dati possono essere copiati accedendo alla memoria tramite una sequenza chiave segreta. I keylogger hardware sono molto efficaci in quanto la loro installazione è molto semplice e il sistema non è in grado di accorgersi della loro presenza, infatti non c'è necessità di alcun software installato sul sistema operativo del computer da monitorare, di conseguenza il dispositivo risulta invisibile ai software antivirus. Quando installati fra la tastiera e il PC hanno le sembianze di un adattatore o appaiono come dei cavi di prolunga. Quando sono nascosti nella tastiera risultano del tutto invisibili (ADAM PASH, *Keep your passwords safe at public computers*, in *Lifehacker*, 9 maggio 2016).

[5] Sul punto si segnala la recente decisione adottata nei confronti dal fratelli Occhionero, Cass., Sez. V, 20 ottobre 2017, n. 48370, *inedita*, con la quale è stata riconosciuta oltre alla riconosciuta legittimità della funzione di intercettazione tra presenti anche l'utilizzabilità dei dati captati dal *trojan* grazie alla modalità di captazione dei flussi comunicativi o comunque oggetto di intercettazioni telematiche cifrate non intellegibili che grazie al *trojan* però possono essere acquisiti in chiaro (anche se in parte).

Se si pensa che in futuro il monitoraggio potrebbe non limitarsi a cellulari e pc, ma estendersi a tutti gli oggetti smart — dalla tv all'auto — lo scenario diventa orwellianamente preoccupante.

Insomma, il tema è particolarmente delicato poiché i captatori non distinguono l'attività criminale dalla vita di tutti i giorni consentendo di fatto a soggetti esterni di prendere possesso della vita digitale di tutti, ponendo a rischio la privacy e la vita personale della collettività.

Da ciò la necessità di approfondire il problema in chiave squisitamente tecnica e di fissare una sorta di "statuto" delle intercettazioni ambientali mediante utilizzo del *trojan* in tutte le ipotesi specificamente individuabili.

A tal uopo si può effettuare la seguente schematizzazione: *a)* intercettazione di comunicazioni tra presenti, in procedimenti diversi da quelli relativi a criminalità organizzata, in luoghi rientranti nella previsione di cui all'art. 614 c.p. nei quali si stia svolgendo l'attività criminosa; *b*) intercettazione di comunicazioni tra presenti, in procedimenti diversi da quelli relativi a criminalità organizzata, in luoghi diversi da quelli *ex* art. 614 c.p.

Ora, se è esclusa, *de iure condito*, la possibilità di intercettazioni nei luoghi indicati dall'art. 614 c.p. con il mezzo del captatore informatico, avendo sempre come riferimento una richiesta del pubblico ministero di disporla in tutti i luoghi in cui si trova il dispositivo informatico portatile preventivamente infettato (perché, occorre ricordare ancora, è stata proprio questa la questione storicamente pruriginosa), ciò discende da due condivisibili argomenti: da un lato la necessità di un adeguato controllo del giudice al momento dell'autorizzazione; dall'altro l'esigenza di mitigare il rischio di una pluralità di intercettazioni tra presenti in luoghi di privata dimora.

Il che porterebbe, di contro, a ritenere pienamente legittime, quantomeno le intercettazioni di comunicazioni tra presenti mediante utilizzo del *trojan*, in procedimenti diversi da quelli relativi a criminalità organizzata, in luoghi rientranti nella previsione di cui all'art. 614 c.p. e nei quali si stia svolgendo l'attività criminosa, ove preventivamente indicati (in termini precisi) nella richiesta di intercettazione; le intercettazioni di comunicazioni tra presenti tramite utilizzo del *trojan*, in procedimenti diversi da quelli relativi a criminalità organizzata, in luoghi diversi da quelli *ex* art. 614 c.p., allo stesso modo preventivamente indicati (ma qui anche semplicemente in termini generici di "ambiente") nella richiesta di intercettazione.

In entrambi i casi sembrano infatti poter essere rispettati non solo i principi di garanzia dell'individuo ma — ancor prima — sussistenti tutti i relativi presupposti tecnico-investigativi.

3. Le perquisizioni informatiche atipiche.

Sulla scorta delle premesse di cui innanzi, bisogna necessariamente distinguere tra l'ipotesi in cui il trojan venga usato per effettuare intercettazioni ambientali[6] dal suo impiego per perquisire a distanza gli archivi di computer, tablet, smartphone. Sotto quest'ultimo aspetto è chiaro che l'ipotesi fuoriesce dal raggio d'azione degli art. 14 e 15 Cost. e, dunque, non basterebbe una disciplina normativa ma sarebbe necessaria l'affermazione di un nuovo (ed inedito) diritto fondamentale all'uso libero e riservato delle tecnologie informatiche. Non consistendo in una intrusione fisica in una privata dimora, infatti, le perquisizioni on-line non minacciano il domicilio.

Frugare fra i file contenuti in un hard disk, inoltre, è attività diversa dal carpire il flusso di una corrispondenza o di un dialogo in atto, che non lede la libertà e la segretezza delle comunicazioni. In questa prospettiva, è stata indicata a modello l'elaborazione della Corte costituzionale tedesca che, in una nota sentenza del febbraio 2008, ha sancito un apposito diritto fondamentale ("il diritto all'uso riservato e confidenziale delle tecnologie informatiche"), derivato dalla dignità della persona, matrice dei diritti fondamentali[7].

Tuttavia, non sempre è agevole comprendere quale mezzo tecnologico sia stato impiegato nella specifica indagine e, dunque, procedere alla relativa qualificazione giuridica.

---

[6] ORLANDI, *Osservazioni su documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Arch. pen.* (web), luglio 2016.

[7] Si tratta della sentenza del Bundesverfassungsgericht 27 febbraio 2008, in *Riv. trim. dir. pen. econ.*, 3, 2009, p. 679 ss., con nota di FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung*, con la quale è stata riconosciuta l'inadeguatezza dei diritti a tutela delle libertà di domicilio e delle comunicazioni a dare copertura sufficiente allo spazio digitale, ed è stato inaugurato un nuovo diritto costituzionale riconducibile alla c.d. "autodeterminazione informativa" e "sicurezza informatica", quest'ultima da intendersi anche come integrità e riservatezza dei dati e delle informazioni trattate da sistemi informatici, fondato sulla dignità umana dell'individuo e dell'utente "informatico". Nel 2016 è intervenuta un'altra pronuncia (Bundersverfassungsgericht, I Senato, 20 aprile 2016, 1 BVR 966/09, 1 BVR 1140/09, in *Cass. pen.*, 8 maggio 2016, sulla quale sia consentito il rinvio a GIORDANO-VENEGONI, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, con la quale è stato ribadito che, anche nel caso di investigazioni compiute per mezzo di strumenti tecnologici che garantiscono l'accesso da remoto ai sistemi informatici, va garantito il nucleo della vita privata ("Kernbereich privater Lebensgestaltung" nella versione originale tedesca, "core area of private life", nella traduzione inglese del comunicato stampa della Corte), non tutelato adeguatamente, secondo la Corte, dal paragrafo 20k della legge federale denominata "Bundeskriminalamtgesetz" – BKAG – che disciplina i compiti e l'attività della forza di polizia federale, la quale prevede il controllo dei dati raccolti ad opera del personale dell'ufficio federale di polizia penale e non di soggetti esterni e indipendenti. Al riguardo, infatti, va segnalato che la disciplina delle intercettazioni in Germania è caratterizzata dall'intangibilità assoluta del nucleo caratterizzante la vita privata e dal controllo politico-parlamentare (cfr. RUGGERI, *Le intercettazioni e la sorveglianza di comunicazioni e dati nei Paesi di area tedesca*, in AA.VV., *Le intercettazioni di conversazioni, Un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti, Atti del Convegno dell'Associazione tra gli studiosi della procedura penale*, Milano, 2007, p. 218).

L'osservazione rimanda ad una significativa decisione della Suprema Corte che permette di cogliere la portata del problema[8].

Nel corso di un'indagine relativa ad un'organizzazione che importava ingenti quantitativi di cocaina dal Sud-America veniva captata la corrispondenza elettronica di diversi imputati[9]. Le e-mail, in particolare, erano oggetto di un provvedimento d'intercettazione di flussi telematici in entrata e in uscita dai computer ubicati nei predetti internet point ai sensi dell'art. 266-bis c.p.p. Le comunicazioni lasciate in "bozza" e quelle che erano state inviate o ricevute in precedenza, ma giacenti nelle diverse cartelle dell'account, venivano carpite con un sistema più ingegnoso: gli investigatori si procuravano le credenziali di accesso controllando a distanza gli imputati tramite trojan che, inoculato nei computer, permetteva di conoscere quanto veniva digitato sulla tastiera; quindi, entravano direttamente nelle caselle di posta elettronica, apprendendone il contenuto.

La Corte, nella specie, ha ritenuto che le e-mail pervenute o inviate al destinatario ed archiviate nelle cartelle della posta elettronica (cioè "parcheggiate") possono essere oggetto di intercettazione, trattandosi di un flusso di dati già avvenuto ed essendo irrilevante la mancanza del presupposto della loro apprensione contestualmente alla comunicazione. Esulano, invece, dal materiale intercettabile le e-mail "bozza", non inviate al destinatario", ma conservate nell'account di posta (o in apposito spazio virtuale come Dropbox[10] o Google Drive[11]), le quali possono comunque

---

[8] Cass., Sez. IV, 28 giugno 2016, n. 40903, in *CED Cass.*, n. 268228.

[9] Più specificamente, durante le investigazioni, per mezzo di servizi di pedinamento e osservazione, era stato appurato che gli imputati frequentavano alcuni internet point di Roma per accedere ad alcune caselle di posta elettronica attivate presso il provider statunitense "hotmail.com", con le quali intrattenevano una corrispondenza con i complici sudamericani. I contatti informatici avvenivano secondo due diverse modalità. In alcuni casi, i messaggi di posta erano normalmente spediti in via telematica; in altri, invece, venivano scritte e-mail che non erano inoltrate al destinatario, ma archiviate nella cartella "bozze". Esse potevano essere lette dai complici che, in possesso di username e password, accedevano successivamente alla casella di posta elettronica. Questo singolare modo di comunicare era impiegato soprattutto per le informazioni più riservate, come quelle che avevano ad oggetto i numeri telefonici "dedicati" allo svolgimento delle singole operazioni di importazione di droga.

[10] Dropbox è un servizio di file hosting gestito dalla società americana Dropbox Inc., che offre cloud storage, sincronizzazione automatica dei file, cloud personale e software client. Esso si basa sul protocollo crittografico Secure Sockets Layer (SSL), i file immagazzinati e accessibili tramite password vengono cifrati tramite AES con chiave a 256 bit. Il programma per usufruire del servizio, scaricabile gratuitamente, è disponibile per Windows, macOS, Linux, iOS, BlackBerry OS, Android, Windows RT e Windows Phone. Il meccanismo utilizza un modello di business freemium, dove viene offerto un account gratuito con una capacità di 2 GB di base, estendibili, in vari modi, fino a 18 GB in totale. Ad esempio, si guadagnano 500 MB per ogni nuova persona invitata che si registri al sito e installi il software sul proprio computer. È possibile aumentare ulteriormente lo spazio gratuito collegando il proprio account ai social network (fino a 640 MB) oppure usando le versioni beta del programma (fino a 5 GB). I piani tariffari a pagamento permettono di aumentare lo spazio fino a 1 TB e di guadagnarne altro invitando nuove persone a utilizzare il servizio. Il servizio può essere usato anche via web, caricando e visualizzando i file tramite il browser, oppure tramite il driver locale che sincronizza automaticamente una cartella locale del file system con quella condivisa, notificando le sue attività all'utente. L'interfaccia web consente il caricamento di file con dimensione massima pari a 300 MB ciascuno. I link che utilizzano più di 20 GB/giorno per account di base (gratis) e 200 GB/giorno per account Pro e Business (a pagamento) vengono

essere acquisite per mezzo di un sequestro di dati informatici. Tra i vari spunti che la decisione suscita meritano di essere approfonditi proprio i limiti connessi all'impiego del virus tipo trojan.

Secondo la sentenza in disamina, infatti, «l'uso del trojan…è stato limitato…all'acquisizione delle password di accesso agli account di posta elettronica. Ottenute queste password, gli inquirenti hanno avuto anch'essi accesso ai vari account nomeutente@hotmail.com e hanno preso visione: a) dei messaggi che venivano via via inviati o ricevuti; b) dei messaggi che venivano salvati nella cartella "bozze"». Di conseguenza, «si è usato il programma informatico…così come si è da sempre usata la microspia per le intercettazioni telefoniche o ambientali».

Su questo punto appare legittimo dissentire.

Non sembra, invero, che il software sia stato adoperato per cogliere comunicazioni, quanto piuttosto per individuare ciò che era digitato sui computer. In questo modo sono state acquisite le password che hanno consentito l'accesso agli

---

automaticamente sospesi. Nel novembre 2009 Dropbox raggiunge la cifra di 3 milioni di utenti, e il 20 gennaio 2010 annuncia il raggiungimento di 4 milioni di utenze. Il 13 novembre 2012 Dropbox ha raggiunto 100 milioni di utenti. Dal 10 gennaio 2014 al 13 gennaio 2014 Dropbox ha sofferto un downtime, che inizialmente ha coinvolto oltre alla sincronizzazione via app anche il sito, al 12 gennaio il problema ha riguardato sia la webapp, questo è stato risolto il 12 gennaio 2014, mentre il problema alla sincronizzazione è durato più a lungo. A detta dello staff il problema si è verificato durante una manutenzione programmata del sistema dove a causa di un baco in uno script di aggiornamento alcuni dei sistemi critici sono andati offline ed è stato necessario ripristinarli con un backup in quanto le macchine di riserva erano anch'esse compromesse (cfr. ROBIN WAUTERS, *Dropbox Announces 4 Million Users, Hires A VP From Salesforce*, in *TechCrunch*, 20 gennaio 2010; MIKE SCHRAMM, *Dropbox hits 100 million users, looking for great Dropbox stories*, in *Engadget*, 14 novembre 2012).

[11] Google Drive è un servizio, in ambiente cloud computing, di memorizzazione e sincronizzazione online introdotto da Google il 24 aprile 2012. Il servizio comprende il file hosting, il file sharing e la modifica collaborativa di documenti, inizialmente fino a 5 GB, da ottobre 2013, invece fino a 15 GB gratuiti (inclusivi dello spazio di memorizzazione di Gmail e delle foto di Google+) estendibili fino a 30 TB in totale. Il servizio può essere usato via web, caricando e visualizzando i file tramite il web browser, oppure tramite l'applicazione installata su computer, che sincronizza automaticamente una cartella locale del file system con quella condivisa. Su Google Drive sono presenti anche i documenti creati con Google Documenti. La peculiarità dell'applicazione è di risiedere sul server Google e di essere lanciata da remoto, non richiedendo l'installazione di alcun software sul computer locale. Diversamente da altri applicativi che lavorano da remoto, nemmeno i dati sono salvati in locale. Questo consente di condividere i file con altri utenti invitati con diversi livelli di privilegio (sola lettura, accesso in scrittura ad alcune parti o a tutto il documento) e di utilizzare i file da qualunque computer tramite cui ci si colleghi alla casella di posta. La conservazione dei dati non in locale pone però seri problemi di privacy per le aziende e per i singoli, sia per l'utilizzo delle informazioni a scopo di schedature che potrebbe essere fatto da chi gestisce il servizio, sia per il maggiore rischio di attacchi e manipolazioni da parte di soggetti esterni, che si verifica quando i dati risiedono su server sempre connessi a Internet. Esiste una policy di sicurezza, ma le legislazioni nazionali sulla privacy non sono allineate verso uno standard internazionale. La cifratura dei dati e l'adozione di protocolli di comunicazione sicura (come SSL) contribuiscono a ridurre il rischio di attacchi esterni, ma non garantiscono un utilizzo appropriato delle informazioni (cfr. JOSH SMITH, *What you love about Google Search—now for Drive*, in *The Keyword Google Blog. Google.*, September 20, 2016, Retrieved November 12, 2016; NAPIER LOPEZ, *Android users can now find Google Drive files right in Search*, in *The Next Web*, February 23, 2017, Retrieved March 27, 2017).

account[12] di posta elettronica ed alle mail contenute[13]. Appare arduo, insomma, ricomprendere la digitazione sulla tastiera di un computer necessaria per accedere ad una casella di posta elettronica nel concetto di comunicazione. Sembra piuttosto che il software sia stato usato per compiere un'ispezione o una perquisizione, di tipo elettronico[14], che ha condotto all'acquisizione (sequestro) della password, attività con le quali il legislatore non si è appieno confrontato.

---

[12] Attraverso il meccanismo dell'account, il sistema mette a disposizione dell'utente un ambiente con contenuti e funzionalità personalizzabili, oltre ad un conveniente grado di isolamento dalle altre utenze parallele. Il termine deriva dal gergo bancario, ed infatti in molte lingue la stessa parola indica un conto corrente ed un conto in banca, ad esempio in lingua inglese (account, parola presa in prestito in italiano) o polacco (konto), quasi ad evidenziare la possibilità di usufruire di servizi che ha un utente registrato ed identificato presso un sito web (paragonabile ai servizi del cliente che ha mostrato il proprio documento presso la sua banca). Infatti, il sistema informatico è in grado di riconoscere l'identità del titolare di un account, ne memorizza e conserva un insieme di dati ed informazioni attribuite ad esso, spesso da esso unicamente gestibili ed accessibili per un utilizzo futuro. In questo si differenzia da altre modalità di accesso a sistemi di servizio interattivi che non presuppongono la ripetizione del rapporto con l'utente. L'insieme di dati e informazioni che individuano il titolare dell'account nonché le preferenze di utilizzo, rappresentano il profilo associato all'account. L'accesso a un account è un processo chiamato login (o logon) ed associato ad una procedura di riconoscimento, detta autenticazione. Durante l'autenticazione, sono richieste le credenziali d'accesso, cioè il nome utente (username) e la relativa password (parola d'ordine o chiave d'accesso). Tali credenziali possono essere definite manualmente da un amministratore o generate automaticamente attraverso un processo di registrazione denominata signup. Lo username dovrebbe essere tale da consentire un riconoscimento univoco dell'utenza. Non è impossibile, tuttavia, che ad una singola utenza sia associata una pluralità di username. L'username, frequentemente, è conoscibile in forma pubblica, ed è sempre noto all'amministratore del sistema. La password, invece, è un'informazione rigorosamente attribuita al possesso dell'utente, che ne è unico responsabile. Allo scopo, viene conservata dal sistema in forma criptata non reversibile (funzione di hash). Può essere sovrascritta in qualunque momento dall'amministratore con una nuova password, senza che questa azione permetta allo stesso amministratore di risalire alla password originale. Questo ha significato se si pensa che l'utente per ricordare le password a memoria avrà delle preferenze nella scelta delle sue chiavi che per questioni di sicurezza è bene non siano individuate da persone estranee (anche se si tratta di un amministratore). La complessità delle funzionalità richieste al processo di accesso impone di affidarne la gestione a veri programmi autonomi. Quelli con interfaccia grafica sono chiamati desktop manager. Tra i principali si possono citare kdm e gdm, che implementano, tra le altre cose, degli strumenti di configurazione molto flessibili, basati su tecnologie xml, l'autologin, un menu con la lista degli utenti, un menu con la lista degli ambienti desktop e dei gestori grafici disponibili, uno strumento per l'accesso remoto a servizi remoti in ascolto, come l'XDMCP e via dicendo.

[13] Nel caso di specie, dunque, l'acquisizione del flusso informativo non è avvenuto mediante la duplicazione della casella di posta elettronica da parte del gestore, con il conseguente inoltro di tutte le email al server della Procura della Repubblica, ma penetrando all'interno della casella di posta elettronica grazie all'acquisizione delle credenziali. In questo modo, sono state carpite mail in un account di posta elettronica @hotmail.com gestita da una società statunitense, il cui server è allocato in territorio americano e che, verosimilmente, avrebbe potuto porre ostacoli agli investigatori. Sull'acquisizione delle e-mail si veda MANCUSO, *L'acquisizione di contenuti e-mail*, in Scalfati (a cura di), *Le indagini atipiche*, Torino, 2014, p. 53.

[14] Con la legge 18 febbraio 2008 n. 48 lo Stato italiano ha ratificato e dato esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23 novembre 2001, e ha così aggiornato alcune norme del III e del IV libro del codice di procedura penale concernenti le prove e le indagini, consentendo ispezioni, perquisizioni, sequestri e accertamenti urgenti di PG riguardo a sistemi o programmi informatici e telematici, anche se salvaguardati da misure di sicurezza. La nuova normativa

non ha regolamentato nel dettaglio le operazioni di acquisizione di notizie informatiche, ma ha indicato pragmaticamente quale debba essere il risultato finale da conseguire piuttosto che il metodo per raggiungerlo, evitando così una scelta fra vari possibili protocolli che, come s'è già detto, sono innumerevoli e soggetti a frequentissimi aggiornamenti in conseguenza dell'evoluzione continua della disciplina. Il legislatore ha invece indicato la necessità di soddisfare alcune esigenze dirette a: consentire la conservazione dei dati originali; impedirne l'alterazione nel corso delle operazioni di ricerca delle fonti di prova; garantire la conformità della copia all'originale, nonché la sua immodificabiltà quando si proceda ad una duplicazione; dotare di sigilli informatici i documenti appresi. Le modifiche apportate dalla legge n. 48 del 2008 hanno riguardato alcuni punti del codice di procedura penale: in tema di ispezioni, all'art. 244 comma 2 secondo periodo sono state aggiunte le parole: "anche in relazione a sistemi informatici, telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione"; all'art. 247, che concerne casi e forme delle perquisizioni, è stato inserito il comma 1 bis: "Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché non protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione"; è stato sostituito il primo comma dell'art. 254, riguardante il sequestro di corrispondenza, col seguente: "Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato"; è stato aggiunto l'art. 254 bis : "Sequestro di dati informatici presso fornitori di servizi informatici, telematici o di telecomunicazioni. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei servizi medesimi, che la loro acquisizione avvenga mediante la copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali"; nel primo comma dell'art. 256, che riguarda il dovere delle persone indicate dagli artt. 200 e 201 di consegnare immediatamente atti e documenti, sono state aggiunte le parole: "nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto"; al secondo comma dell'art. 259, riguardante gli obblighi del custode delle cose sequestrate, è stato aggiunto il periodo: "Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria"; l'art. 260 prevede ora che il sigillo alle cose sequestrate possa essere apposto con mezzi "anche di carattere elettronico o informatico"; nell'art. 352, che riguarda le perquisizioni a iniziativa della polizia giudiziaria, è stato inserito il comma 1 bis: "Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi"; l'art. 353 prevede che il pm autorizzi la pg a ricercare notizie utili all'assicurazione delle fonti di prova non solamente con l'immediata apertura di plichi, ma anche con l'"accertamento del contenuto" della corrispondenza informatica; dopo il primo periodo dell'art. 354 ("accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro") è stato aggiunto: "In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informativi o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurare la conservazione e a impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità". Le garanzie indicate dalla novella del 2008 hanno l'evidente finalità di assicurare l'acquisizione di elementi di prova genuini e attendibili e di raggiungere l'obbiettivo

Il tema, allora, rimanda alle affermazioni di diritto rese sull'argomento dal Supremo organo nomofilattico.

4. La sentenza "Scurato".

Con la sentenza n. 26889 del 28 aprile 2016, Scurato[15], le Sezioni Unite della cassazione, come è noto, hanno affrontano il tema dell'impiego, per lo svolgimento di intercettazioni, di programmi informatici inseriti a distanza in apparecchi elettronici come smartphone, computer o tablet.

Tra le diverse azioni astrattamente realizzabili con un software che presenta le potenzialità descritte, la decisione si sofferma solo sul suo impiego allo scopo di ascoltare dialoghi tra presenti.

Questa, infatti, è la sola attività investigativa che è stata esperita nella vicenda posta al vaglio della Suprema Corte e che, di conseguenza, è stata oggetto di eccezione di inutilizzabilità.

---

di salvaguardare, a tutela dei diritti della difesa, la possibilità del controllo successivo dell'attività degli inquirenti, che deve concernere in primo luogo la verifica del metodo utilizzato per l'acquisizione. I procedimenti scientifici riguardanti l'informatica e la raccolta della prova digitale, come detto, sono in continua evoluzione. È sorto in passato il dubbio che, in relazione alla novità che le riguardano, l'assunzione di quelle emergenze probatorie dovesse ritenersi regolata dall'art. 189 cpp, cioè dalla norma nata sia per disciplinare situazioni contrassegnate da caratteristiche di novità, che per evitare eccessive limitazioni all'accertamento della verità in relazione al "continuo sviluppo tecnologico che estende le frontiere dell'investigazione", richiamato dalla Relazione al progetto preliminare del cpp. L'applicazione della disciplina dettata dal citato art. 189 implica che il richiedente dimostri l'idoneità della prova atipica ad accertare i fatti, anche in relazione alla "affidabilità dei metodi e delle procedure adottate dall'esperto". È sorto però il dubbio che quella norma potesse riguardare esclusivamente gli strumenti scientifici nuovi o controversi (accertamento che lascerebbe uno spazio eccessivo alla discrezionalità in relazione alla definizione dei detti requisiti), sia perché essa non contiene un'indicazione specifica in tal senso, sia perché quella regolamentazione potrebbe essere applicabile anche ad altri collaudati mezzi di prova scientifica il cui svolgimento non sia però regolato dalla legge. La novella del 2008 ha ricondotto le attività di ricerca e raccolta della prova informatica nel novero dei mezzi tipici disciplinati dal codice con la conseguenza che anche riguardo all'ammissione delle prove informatiche si applicano le regole dettate dall'art. 190 cpp. Da ciò consegue che una prova che sia fondata su teorie o procedimenti scientifici inaffidabili non può essere ammessa poiché "la prova non autenticamente scientifica è manifestamente irrilevante". Nel momento dell'assunzione il giudice deve valutare criticamente l'affidabilità delle procedure e dei metodi scientifici adottati dagli inquirenti sulla base di alcuni criteri fondamentali che sono generalmente indicati nella "accettazione generale da parte degli studiosi… dal grado di controllabilità e falsificabilità del metodo scientifico, l'esistenza di una revisione critica da parte degli esperti del settore, l'indicazione del margine di errore conosciuto…". Naturalmente, vertendosi in tema di prova, è necessario che chi intenda contraddire un elemento istruttorio offerto dalla parte avversa si debba addossare l'onere di indicare gli elementi sui quali si basa l'eccezione. La difesa che contesti gli elementi di prova informatica portati dal pm deve specificare i dati di fatto in cui si sostanzi la violazione e deve fornire gli elementi di giudizio che la facciano ritenere sussistente. È necessario quindi che la parte interessata segnali, e alleghi, protocolli, linee guida, regole tecniche comunemente accettate dagli ambienti scientifici che ritiene siano stati violati nel corso della raccolta della prova e abbiano determinato una qualche distorsione del dato informatico.

[15] In *Guida dir.*, 2016, 30, p. 87.

Orbene, secondo la decisione, anche se eseguite con mezzo informatico, le intercettazioni compiute per mezzo dell'agente intrusore vanno ricondotte a quelle di natura ambientale disciplinate dall'art. 266, comma 2, c.p.p. Esse, però, presentano una caratteristica peculiare: se il programma è installato in un dispositivo portatile possono avvenire in qualsiasi luogo sia condotto detto mezzo, dunque anche in un domicilio. Proprio tale potenzialità operativa comporta la necessità di realizzare un difficile bilanciamento delle esigenze investigative con la garanzia dei diritti individuali alla riservatezza, all'inviolabilità del domicilio ed alla segretezza delle comunicazioni.

Di tal che, dopo aver delineato le caratteristiche dello strumento investigativo in esame, le Sezioni unite hanno individuato la disciplina applicabile nella specie in quella delle intercettazioni "ambientali", richiamando gli artt. 266, 267 e 271 c.p.p. nonché, tenuto conto che all'indagato era contestato un reato di criminalità organizzata, l'art. 13 del decreto legge n. 152 del 1991, convertito dalla legge n. 252 del 1991.

Ad ogni modo, secondo la Corte, anche in forza di una lettura orientata dalle disposizioni costituzionali e convenzionali, l'art. 266, comma 2, c.p.p. non imporrebbe come condizione di legittimità di un provvedimento di intercettazione "ambientale" la precisazione dello specifico luogo in cui deve essere svolta l'attività investigativa.

In questo senso, dunque, le Sezioni Unite manifestano di non condividere l'orientamento dalla sentenza Musumeci[16], secondo la quale l'intercettazione delle conversazioni tra presenti sarebbe da ritenersi legittima solo se il relativo decreto autorizzativo individua con precisione i luoghi in cui eseguire tale attività captativa. La specificazione del "dove" nel provvedimento autorizzativo, invece, sarebbe necessaria soltanto quando la captazione deve intervenire nei luoghi indicati nell'art. 614 c.p. Esclusivamente in questo caso, infatti, l'art. 266, comma 2, c.p.p. prevede come condizione di legittimità delle intercettazioni da realizzarsi in luoghi di privata dimora il «fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa».

Ne deriva che, in detta ipotesi, è indispensabile la puntualizzazione del domicilio in cui si deve svolgere l'intercettazione perché bisogna che nel posto individuato sia in corso l'attività criminale.

Al riguardo, la Corte precisa che l'espressione "intercettazioni ambientali" è invalsa nella prassi in un'epoca in cui questo genere di captazioni aveva bisogno dell'apposizione di una "micro-spia" in un preciso ambiente. Il codice di rito, invece, utilizza la più precisa locuzione di intercettazioni «tra presenti», a riprova del fatto che, di regola, la determinazione del luogo in cui avvengono le rilevazioni non è un presupposto di legittimità del provvedimento.

Dalla disciplina delle intercettazioni "tra presenti" così ricostruita, la decisione trae le dirette conseguenze sull'impiego del cd. captatore informatico installato su di un apparecchio portatile: nel momento in cui autorizza un'intercettazione da effettuarsi in tale modo, «il giudice non può prevedere e predeterminare i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto». Ciò comporta che non

[16] Cass., Sez. VI, 26 maggio 2015, n. 2710, in *C.E.D. Cass.*, n. 265654.

potrebbe esperirsi un adeguato controllo circa l'effettivo rispetto del presupposto di legittimità previsto dall'art. 266, comma 2, c.p.p., non potendo appurarsi che nel domicilio in cui potrebbe essere condotto l'apparecchio "infettato" sia in corso un'attività criminosa.

Viepiù, la Corte specifica che, anche se fosse possibile seguire gli spostamenti dell'utilizzatore del dispositivo elettronico, sospendendo la captazione nel caso di ingresso in un luogo di privata dimora, «sarebbe comunque impedito il controllo del giudice al momento dell'autorizzazione, che verrebbe disposta al buio», cioè senza aver valutato preventivamente che in detto posto sia in atto un'attività criminosa.

5. Le valutazioni imposte dalla sentenza "Scurato".

Di primo acchito sembra doversi manifestare un giudizio negativo rispetto alle conclusioni della sentenza in oggetto perché né il codice di procedura penale, né altre leggi autorizzano l'uso di un mezzo tanto invasivo. Gli artt. 14 e 15 Cost. e l'art. 8 CEDU richiedono la specifica previsione di legge per ogni violazione dell'intimità domiciliare e della segretezza delle comunicazioni nonché per ogni ingerenza dell'autorità pubblica nella vita privata e familiare degli individui. La necessità di contrastare la criminalità, in particolare quella organizzata e terroristica, con i più sofisticati strumenti di indagine, dunque, non è sufficiente per superare la preoccupazione che ingenera l'uso di tali strumenti di intrusione informatica in mancanza di specifiche disposizioni normative che regolino la materia nell'adeguato bilanciamento dei principi costituzionali e convenzionali coinvolti.

Sotto diverso profilo, però, potrebbe rilevarsi che, proprio come evidenziato della sentenza della Suprema Corte, l'uso della tecnica in esame per effettuare intercettazioni "tra presenti" trovi una base legale negli artt. 266 e 266-bis c.p.p. e nell'art. 13 del d.l. n. 152 del 1991.

L'impiego per altre finalità come la perquisizione a distanza degli archivi di computer, tablet, smartphone, invece, sarebbe privo di un fondamento giuridico, fuoriuscendo dal raggio di azione degli artt. 14 e 15 Cost.

L'intervento del legislatore, pertanto, si è rivelato quanto mai imprescindibile nella specie soprattutto in relazione allo specifico profilo delle cd. perquisizioni on-line (che, comunque, esulava dall'ambito del giudizio di cui erano investite le Sezioni unite). Rispetto a questo aspetto apparendo essenziale l'affermazione di un nuovo (ed inedito) diritto fondamentale all'uso libero e riservato delle tecnologie informatiche.

Dopo la decisione illustrata, peraltro, il tema è stato affrontato solo da poche pronunce.

Alcune sentenze della Sezione Sesta, tutte nondimeno concernenti la medesima vicenda cautelare che ha dato l'occasione per l'intervento delle Sezioni Unite, hanno ribadito che è ammissibile l'utilizzo del captatore informatico limitatamente ai procedimenti relativi a delitti di criminalità organizzata, anche terroristica, a norma

dell'art. 13 del decreto legge n. 152 del 1991, intendendosi per tali quelli elencati nell'art. 51, comma 3-bis e 3-quater, c.p.p.[17]

L'eccezione di inutilizzabilità delle intercettazioni compiute per mezzo del software, inoltre, è stata formulata in un giudizio avente ad oggetto reati di corruzione, falso, turbativa d'asta, truffa ed altro[18].

In questo caso, la Corte, pur dando atto in motivazione dell'intervenuto pronunciamento delle Sezioni Unite che limita la possibilità di impiegare il cd. captatore informatico ai reati di criminalità organizzata, ha ribadito l'orientamento consolidato secondo il quale è onere della parte che lamenti l'inutilizzabilità dei risultati delle intercettazioni indicare con precisione l'atto asseritamente affetto dal vizio denunciato e curare e che lo stesso sia acquisito al fascicolo trasmesso al giudice di legittimità, anche provvedendo a produrlo in copia nel giudizio di cassazione[19].

Il mancato adempimento di tale onere ha determinato il rigetto dell'eccezione.

6. Il *trojan* e la nozione di "criminalità organizzata".

Dal momento in cui è stato reputato legittimo l'impiego del virus autoinstallante per la realizzazione di intercettazioni "tra presenti" limitatamente ai delitti di "criminalità organizzata"[20], il tema si è spostato sulla nozione di "criminalità organizzata".

Nel nostro ordinamento non esiste una definizione di criminalità organizzata. La accezione può essere ricavata solo da elementi criminologici, sociologici o dalle convenzioni internazionali che si sono occupate della materia ed in primo luogo dalla Convenzione TOC (Transnational Organized Crime), Convenzione ONU, siglata a Palermo nel dicembre del 2000 e ratificata nel nostro ordinamento con la 1. n. 146 del 2006.

A differenza di tutti gli altri ordinamenti di civil law ovvero di common law, il sistema italiano conosce cinque varianti di criminalità organizzata: a) la criminalità organizzata comune, ovvero quella riconducibile allo schema dell'associazione per delinquere prevista dall'art. 416 c.p., che si riscontra in tutti i casi nei quali un gruppo

---

[17] Cfr. Cass., Sez. VI, 3 maggio 2016, sent. n. 27404, Marino, *inedita*; Cass., Sez. VI, 3 maggio 2016, sent. n. 26054, Di Cara, *inedita*; Cass., Sez. VI, 3 maggio 2016, sent. n. 26055, Bronte, *inedita*; Cass., Sez. VI, 3 maggio 2016, sent. n. 26058, Lo Iacono, *inedita*.

[18] Cass., Sez. V, 4 marzo 2016, n. 26817, Iodice ed altri, *inedita*

[19] Cfr. Cass., Sez. II, 11 aprile 2013, n. 24925, in *C.E.D. Cass.*, n. 256540.

[20] Secondo la decisione, per questo genere di reati, l'installazione del captatore informatico in un dispositivo "itinerante" costituisce «una delle naturali modalità di attuazione delle intercettazioni», al pari della collocazione di microspie all'interno di un luogo di privata dimora. Escludendo espressamente il requisito autorizzativo previsto dall'art. 266, comma 2, secondo periodo, c.p.p. il legislatore «ha operato evidentemente uno specifico bilanciamento di interessi, optando per una più pregnante limitazione della segretezza delle comunicazioni e della tutela del domicilio tenendo conto dell'eccezionale gravità e pericolosità, per l'intera collettività, dei (particolari) reati oggetto di attività investigativa per l'acquisizione delle prove».

di persone si associa per la realizzazione di delitti comuni; b) l'associazione di tipo mafioso, disciplinata dall'art. 416-bis c.p., che si concretizza quando il sodalizio pone in essere delitti o addirittura attività lecite (quali il controllo di attività economiche, l'acquisizione di concessioni o appalti, il condizionamento di voti favorevoli durante le competizioni elettorali) attraverso un metodo mafioso, caratterizzato dalla intimidazione e dalla omertà che ne deriva; c) le associazioni c.d. monotematiche, ovvero quelle costituite esclusivamente per la gestione di singole attività delittuose (associazione contrabbandiera, art. 291quater del Testo Unico Leggi Doganali, per il commercio dei tabacchi lavorati esteri, associazione per il traffico di stupefacenti, art. 74 del Testo Unico Stupefacenti, associazione finalizzata alla tratta degli essere umani, art. 416 c.p. sesto comma, ecc.); d) le associazioni con finalità di terrorismo o di eversione dell'ordine democratico, *ex* art. 270 e seguenti codice penale.

Ne deriva un panorama articolato e complesso che ha determinato una serie di deroghe al nostro, sistema processuale.

Occorre considerare, infatti, che sotto il profilo processuale il fenomeno della criminalità organizzata rappresenta soprattutto una conclamata difficoltà per l'acquisizione, della prova.

Sulla base di tali considerazioni il nostro legislatore, nel corso degli anni, ha progressivamente inserito delle deroghe al normale svolgimento delle indagini e del dibattimento processuale, per agevolare il compito degli investigatori e dell'accusa nel contrastare e punire fatti di enorme gravità e di sicuro allarme sociale. Purtroppo, tali modifiche, succedutesi negli anni con una serie di interventi normativi, non costituiscono un complesso organico di norme e non risultano facilmente rinvenibili dall'interprete. Esse, infatti, sono state inserite con commi aggiunti agli articoli del codice, ovvero con provvedimenti contenuti in leggi speciali e, qualche volta, addirittura con modifiche apportate dalla giurisprudenza della Corte` costituzionale o della Suprema Corte di cassazione.

Pertanto, il complesso di tali previsioni può, a ragione, essere definito un "processo di criminalità organizzata" che costituisce un vero e proprio doppio binario all'interno del nostro sistema processuale.

In questa prospettiva, le Sezioni Unite Scurato hanno ribadito la validità dell'approccio "teleologico" o "finalistico" secondo il quale il significato dell'espressione "criminalità organizzata" deve essere definito avendo riguardo alle finalità specifiche della singola disciplina che deroga alle regole processuali generali.

È stata avallata, così, una nozione ampia di "delitti di criminalità organizzata", tale da valorizzare le finalità perseguite dalla norma, le quali mirano a riconoscere uno strumento efficace di repressione dei reati più gravi[21].

[21] La sentenza ha ritenuto di dover confermare la validità di questo indirizzo giurisprudenziale, «perché consente di cogliere l'essenza del delitto di criminalità organizzata e nel contempo di ricomprendere tutti i suoi molteplici aspetti, nell'ottica riconducibile alla *ratio* che ha ispirato gli interventi del legislatore in materia, tesi a contrastare nel modo più efficace quei reati che per la struttura organizzativa che presuppongono e per le finalità perseguite, costituiscono fenomeni di elevata pericolosità sociale».

Sono ricomprese in detta categoria, pertanto, attività criminose eterogenee, purché realizzate da una pluralità di soggetti i quali, per la commissione del reato, abbiano costituito un apposito apparato organizzativo, con esclusione del mero concorso di persone *ex* art. 110 c.p. Ad essa non sono riconducibili solo i reati di criminalità mafiosa, ma tutte le fattispecie criminose di tipo associativo; è sufficiente la costituzione di un apparato organizzativo, la cui struttura assume un ruolo preminente rispetto ai singoli partecipanti.

A tal riguardo, l'aspetto più delicato non appare quello del riferimento agli specifici delitti perseguiti[22], quanto la difficoltà di tracciare un confine sufficientemente delineato tra la fattispecie associativa ed il concorso di persone nella fase delle indagini. Su questa delimitazione si fonda la funzione di garanzia del decreto di autorizzazione[23].

Tale approccio, comunque, deve essere parametrato alla recente "sentenza Romeo"[24].

Per vero, nella motivazione di tale pronuncia la Suprema corte ha significativamente sottolineato che, in considerazione della forza intrusiva del mezzo usato, la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso.

Proprio la particolare invasività dello strumento tecnologico attraverso il quale si concretizzano le modalità di esecuzione di tale mezzo di ricerca della prova, allora, impone un rigoroso apprezzamento, sia nella fase della richiesta che in quella della successiva autorizzazione giudiziale, della solidità della qualificazione dell'ipotesi associativa, che non può essere configurata come una sorta di illecito "contenitore", magari senza una specifica individuazione del ruolo e delle condotte relative ai delitti scopo dell'associazione ipotizzata, strumentalizzandone i tratti identificativi al fine di ottenere l'autorizzazione di intercettazioni per mezzo del captatore informatico, eventualmente da utilizzare ai fini di prova per reati diversi, per i quali non sarebbe stato ammesso l'impiego dello strumento.

7. Gli approdi della "delega Orlando".

L'ampiezza del dibattito sviluppatosi in merito all'utilizzo dei cosiddetti "*trojan*" ha indotto il legislatore ad aggiungere, nel corso dei lavori preparatori della

---

[22] Secondo TESTAGUZZA, Exitus acta probat *"Trojan di Stato"*: *La composizione di un conflitto*, in *Arch. pen.*, 2016, p. 2, in particolare, al fine di delimitare l'ambito di operatività del mezzo tecnologico in esame, «il riferimento ai delitti con finalità di terrorismo…impone una connotazione in via "principale" degli stessi e non anche "accessoria" o meramente "qualificante" come sostenuto dal Supremo consesso».

[23] Cfr., tra le altre, Cass., Sez. II, 14 dicembre 2016, n. 53000, in *C.E.D. Cass.*, n. 268540; Cass., Sez. 4, 16 ottobre 2013 n. 51716, in *C.E.D. Cass.*, n. 257906; Cass., Sez. II, 13 gennaio 2014, n. 933, in *C.E.D. Cass.*, n. 258009.

[24] Cass., Sez. VI, 13 giugno 2017, n. 36874, *inedita*.

riforma Orlando (legge n. 103 del 23 giugno 2017), un ampio principio direttivo, contenuto nel comma 84, lett. e), con cui si è delegato il governo a disciplinare la complessa problematica delle intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in dispositivi elettronici portatili[25].

Sicché, il legislatore delegante non è rimasto sordo all'accorato appello che, dopo la pronuncia da parte delle Sezioni unite della già citata sentenza Scurato[26], molti processual-penalisti hanno rivolto al parlamento affinché intervenisse «con specifiche disposizioni a regolare la materia nell'adeguato bilanciamento dei principi costituzionali e convenzionali coinvolti»[27].

Le indicazioni della delega sul punto sembrano imporre una parziale rilettura del quadro delineato dalla giurisprudenza[28] e, in questa sede, non possono che essere (sommariamente) riassunte.

a) L'attivazione del microfono potrà avvenire solo a seguito di un apposito comando inviato da remoto e non dal mero inserimento del captatore informativo e ciò sempre nel rispetto dei limiti stabiliti da un decreto autorizzativo emanato da un giudice.

b) La registrazione audio dovrà essere avviata dalla polizia giudiziaria o dal personale incaricato su indicazione della polizia operante, la quale sarà tenuta ad indicare necessariamente l'ora di inizio e fine della registrazione, secondo circostanze da attestare nel verbale descrittivo delle modalità di effettuazione delle operazioni di cui all'art. 268 c.p.p.

c) L'attivazione del dispositivo dovrà essere sempre ammessa nel caso in cui si proceda per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. e, fuori da tali casi, potrà essere disposta nei luoghi di cui all'art. 614 c.p. soltanto se negli stessi si stia svolgendo attività criminosa. In ogni caso, il necessario decreto autorizzativo del giudice dovrà indicare le ragioni per le quali tale modalità di intercettazione particolarmente invasiva sia necessaria per lo svolgimento delle investigazioni.

d) Il trasferimento dei file registrati dovrà essere effettuato soltanto verso il *server* della procura e, una volta terminata la captazione, il *trojan* dovrà essere reso definitivamente inutilizzabile.

e) Potranno essere utilizzati soltanto specifici programmi informatici conformi ai requisiti tecnici fissati con decreto ministeriale.

f) Nei casi di urgenza, "il pubblico ministero potrà disporre direttamente tale tipologia di intercettazioni, limitatamente al fatto che si proceda per i delitti di cui all'articolo 51, commi 3-*bis* e 3-*quater*, con successiva convalida da parte del giudice entro 48 ore. Il decreto d'urgenza dovrà dar conto delle specifiche situazioni di fatto che rendono

---

[25] Per un commento assai attento sul punto, cfr. PARODI, *La riforma "Orlando": la delega in tema di "captatori informatici"*, in *www.magistraturaindipendente.it*, 4 aprile 2017.

[26] Cass., Sez. Un., 28 aprile 2016, Scurato, cit.

[27] L'appello si può trovare in *questa Rivista*, 7 ottobre 2016, sotto il titolo *Necessaria una disciplina legislativa in materia di captatori informatici (c.d. "trojan"): un appello al legislatore da parte di numerosi docenti di diritto italiani*.

[28] Cfr. PARODI, *La riforma "Orlando": la delega in tema di "captatori informatici"*, cit.

impossibile la richiesta al giudice, nonché delle ragioni per cui tale insidiosa modalità di intercettazione sia necessaria".
g) Le intercettazioni così ottenute potranno essere utilizzate ai fini probatori soltanto per i reati oggetto del provvedimento autorizzativo e potranno essere utilizzate in procedimenti diversi a condizione che siano indispensabili per l'accertamento di uno dei delitti di cui all'articolo 380 c.p.p.

Come può agevolmente dedursi dalla lettura dei passaggi riportati, gli stessi risentono per intero del dibattito innescato dalla sentenza Scurato delle sezioni Unite.

La delimitazione dell'uso dei trojan nei dispositivi portatili ai soli procedimenti di criminalità organizzata — che la Cassazione aveva segnalato come l'unica consentita — non ha influenzato, comunque, le scelte del Governo.

8. Il decreto attuativo della "delega Orlando".

Venerdì 29 dicembre 2017 il Consiglio dei Ministri ha definitivamente licenziato il Decreto legislativo che riforma la disciplina delle intercettazioni.

Nel proprio comunicato stampa, il Governo ha osservato che "il decreto, nell'attuare una revisione della disciplina delle intercettazioni volta a rendere maggiormente equilibrata la salvaguardia fra interessi parimenti meritevoli di tutela a livello costituzionale, introduce disposizioni volte a incidere sull'utilizzazione, a fini cautelari, dei risultati delle intercettazioni, nonché a disciplinare il procedimento di selezione delle comunicazioni intercettate, secondo una precisa scansione temporale. La finalità è quella di escludere, in tempi ragionevolmente certi e prossimi alla conclusione delle indagini, ogni riferimento a persone solo occasionalmente coinvolte dall'attività di ascolto e di espungere il materiale documentale, ivi compreso quello registrato, non rilevante a fini di giustizia, nella prospettiva d'impedire l'indebita divulgazione di fatti e riferimenti a persone estranee all'oggetto dell'attività investigativa".

Tra le misure principali, il testo fissa una nuova disciplina delle intercettazioni di comunicazioni o conversazioni mediante immissione di captatori informatici in dispositivi elettronici portatili. In particolare, si prevede che tali dispositivi non possano essere mantenuti attivi senza limiti di tempo o di spazio, ma debbano essere attivati da remoto secondo quanto previsto dal pubblico ministero nel proprio programma d'indagine e che, tra l'altro, debbano essere disattivati se l'intercettazione avviene in ambiente domiciliare, a meno che non vi sia prova che in tale ambito si stia svolgendo l'attività criminosa oggetto dell'indagine o che l'indagine stessa non riguardi i delitti più gravi, tra i quali mafia e terrorismo, di cui all'articolo 51, commi 3-*bis* e 3-*quater*, del codice di procedura penale.

Dunque, il decreto darebbe esecuzione alla delega che prevede l'introduzione di una specifica disciplina per l'utilizzo del *trojan* (o captatore informatico) quale strumento di intercettazione delle conversazioni tra presenti.

Si tratta, tuttavia, di un argomento assolutamente differente rispetto alla tutela della *privacy* e la relativa disciplina introduce forti limitazioni che non trovano giustificazione nel diritto alla riservatezza.

Sotto questo profilo, già la citata legge delega aveva operato una sostanziale limitazione dello strumento ai soli reati di mafia e terrorismo lasciando indenni le ulteriori ipotesi di associazione a delinquere disciplinate dall'articolo 416 del c.p., diversamente da quanto in precedenza stabilito dalle Sezioni Unite della Cassazione con la menzionata sentenza del 28 aprile 2016, Scurato.

E però, nel decreto legislativo n. 216 del 2017, a disposizioni fortemente restrittive se ne accompagnano altre di segno opposto, dando l'impressione di un legislatore evidentemente incerto.

Così, in una prospettiva di maggior rigore si prevede che, di regola, l'intercettazione mediante l'impiego di un captatore informatico sia sempre consentita quando si procede per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. (art. 266, comma 2-*bis*, c.p.p.). Indubbia, al riguardo, la limitazione rispetto alle aperture interpretative della sentenza Scurato che consentiva, come detto, il ricorso allo strumento anche per reati "facenti capo ad un'associazione per delinquere ex art. 416 cp, correlata alle attività più diverse, con esclusione del mero concorso di persone".

Qualora si proceda per i delitti di cui all'articolo 51, commi 3-*bis* e 3-*quater*, c.p.p., comunque, lo strumento è utilizzabile anche quando le comunicazioni avvengono nei luoghi indicati dall'art. 614 c.p., senza alcuna previa indicazione degli stessi né limitazioni di tempo. Detto altrimenti, allorquando si procede per uno dei delitti di che trattasi non è necessario che il decreto autorizzativo indichi "i luoghi ed il tempo" in relazione ai quali sia consentita l'attivazione del microfono, e ciò per la assorbente ragione che, per tali reati, l'intrusione anche nei luoghi di privata dimora è consentita a prescindere dalla sussistenza del fondato motivo di ritenere che ivi si stia svolgendo attività criminosa.

In un'ottica di decisa "apertura" rispetto alla sentenza Scurato, il decreto legislativo n. 216 del 2017 consente il ricorso al captatore informatico anche per "reati comuni" (tutti quelli indicati nell'articolo 266, comma 1, c.p.p. non ricompresi tra quelli indicati negli artt. 51, commi 3-*bis* e 3-*quater*, c.p.p.). In siffatte evenienze, in aderenza ai dettami della legge delega, è comunque necessario che il decreto autorizzativo indichi i luoghi ed il tempo, anche indirettamente determinati, in relazione ai quali sia consentita l'attivazione del microfono poiché per le fattispecie in oggetto l'intercettazione nei luoghi indicati dall'art. 614 c.p. è consentita solo laddove ivi si stia svolgendo attività criminosa. A titolo esemplificativo, valga il riferimento a formule del tipo: "ovunque incontri il soggetto x"; "ogni volta che si rechi nel locale y" ecc. ecc.

Ad ogni buon conto, l'intercettazione tra presenti a mezzo di captatore informatico può essere autorizzata in via di urgenza dal pubblico ministero soltanto per i procedimenti concernenti i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. Non è invece consentito un intervento d'urgenza quando si procede per "reati comuni".

Quanto, poi, alla utilizzabilità dei risultati delle intercettazioni rispetto a reati diversi da quelli oggetto di autorizzazione, il materiale acquisito mediante captatore è

impiegabile soltanto per i reati per i quali sia intervenuta valida autorizzazione e non già per la prova dei reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, salvo che risulti indispensabile per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza (art. 270, comma 1-*bis*, c.p.p.). Ovviamente, l'utilizzabilità ai sensi dell'art. 270 c.p.p. presuppone che si tratti di intercettazioni ritualmente autorizzate alle condizioni di legge ed eseguite nel rispetto delle indicazioni del decreto autorizzativo. *Ergo*, non saranno impiegabili le captazioni involontarie effettuate in occasione dell'inserimento del captatore prima ancora che il relativo funzionamento sia stato attivato.

Da un punto di vista meramente operativo, infine, il decreto legislativo in disamina ha novellato la previsione di cui all'art. 89, n. att., c.p.p. imponendo la indicazione nel verbale delle operazioni: del tipo di programma impiegato; dei luoghi di svolgimento delle comunicazioni o conversazioni; della effettuazione delle registrazioni presso il *server* della procura; della disattivazione del captatore, con modalità tali da renderlo inidoneo a successivi impieghi.

A conclusione della esposizione non può non evidenziarsi che dal chiaro tenore della delega e dei sopra menzionati criteri che della stessa ne costituisce attuazione si inferisce come si sia inteso regolamentare soltanto uno degli usi del captatore informatico, quale specifica modalità di esecuzione delle intercettazioni tra presenti.

Lo strumento, infatti, consistendo in un malware «occultamente installato dall'inquirente su un apparecchio elettronico dotato di connessione internet attiva» consente operazioni ulteriori e diverse quali: la captazione del traffico dati (sia in entrata che in uscita); l'attivazione della telecamera installata *ab origine* sul dispositivo; la "perquisizione" degli hard disk; la possibilità di estrarre copia integrale del loro contenuto; la intercettazione di tutto quanto digitato sulla tastiera; la possibilità di fotografare le immagini ed i documenti visualizzati; oltre che consentire la geolocalizzazione del dispositivo.

Si tratta, per vero, di un complesso di operazioni (alcune delle quali già praticate ove consentite dalla legislazione vigente) che la tecnologia consente di effettuare, ma che il legislatore non ha inteso regolare, limitando l'ambito dell'intervento normativo alla disciplina degli aspetti attinenti all'intercettazione audio, eseguita mediante inoculazione di dispositivo portatile (smartphone, tablet ecc.) e non anche di dispositivi fissi.

9. La necessità di una soluzione concreta, a tutela dell'individuo e delle sue prerogative intangibili.

Gli interventi sinora considerati, nonostante gli sforzi profusi nella direzione di "disciplinare" — restringendolo — il ricorso al particolare mezzo captativo in disamina, all'evidenza, si palesano insufficienti sul fronte della tutela delle garanzie individuali.

E tale conclusione è imposta muovendo proprio dalle considerazioni critiche spese a proposito della sentenza Scurato.

Per vero, tale sentenza interviene su richiesta della Sesta sezione, convinta di non poter condividere l'"opinione" di altro ufficio, evocata dalla difesa nei motivi di ricorso, che in precedente occasione aveva ritenuto inutilizzabili i risultati delle "intercettazioni ambientali" ottenute in base ad un decreto autorizzativo privo della indicazione del luogo dove svolgere le operazioni.

In verità, la questione si presenta subito molto più seria e, per le motivazioni espresse dalla stessa giurisprudenza, abbastanza distante dal tema specifico delle intercettazioni. Infatti, la stessa sezione remittente sottolinea la singolarità della vicenda e la (assurda) "pretesa" di indicare con precisione ed anticipatamente i luoghi interessati da una attività captativa, essendo adottata attraverso un dispositivo elettronico "mobile". Eppure, nonostante questa "presa di distanza" — che opportunamente sottolinea i limiti di un (im)possibile analogia con la disciplina delle intercettazioni —, non ci si sottrae dal ritenere questa particolare attività ricompresa nell'ambito delle intercettazioni cd. "ambientali".

Per questa teoria, dunque, il problema del "captatore informatico" è legato esclusivamente ai luoghi di cui all'art. 614 c.p. e, sul piano processuale, solo al controllo successivo; e quindi alla eventuale inutilizzabilità dei risultati, dal momento che la captazione segue lo spostamento del dispositivo e non può essere preventivamente indicato il luogo della captazione.

La tesi è condivisa dalle Sezioni Unite le quali, dopo una approfondita analisi casistica delle diverse posizioni apparse in giurisprudenza, anche di natura sovranazionale, sulla scorta delle specificità "letterali" della disposizione "derogatoria" di cui all' art. 13 dl n. 152 del 1991 (convertito con legge n. 203 del 1991), ricostruiscono il tessuto normativo della vicenda ritenendolo — appunto — derogatorio delle previsioni ordinarie di cui all'art. 266, comma 2, c.p.p., interessandosi — quella norma — di "intercettazioni tra presenti" (non "ambientali"), compiute anche in luoghi di privata dimora, purché inerenti a delitti di "criminalità organizzata".

In particolare si è ritenuto che, per tali delitti il legislatore avrebbe dato "una precisa e significativa indicazione" laddove "avrebbe espressamente escluso, per le intercettazioni tra presenti in privata dimora il requisito autorizzativo previsto dall' art. 266, comma 2, secondo periodo, cod. proc. pen. per tutte le altre intercettazioni, tenendo conto di un contesto temporale in cui la tecnologia non aveva ancora raggiunto l'attuale livello di efficacia e di capacità intrusiva". In questo contesto, dunque, non sarebbe richiesta per il caso di specie la preventiva autorizzazione.

La tesi "autoritária" troverebbe conforto nella giurisprudenza della Cedu, la quale, in verità, offre la misura del sacrificio nella esplicita richiesta della "severità della motivazione" e "della previsione di un impiego rigorosamente circoscritto attraverso previsioni tecniche di utilizzo e limitazioni di ordine giuridico fissate dal giudice ed altrettanto rigorosamente controllato quanto alla fase della esecuzione delle attività captative"[29].

[29] Così si legge a pag. 22 della sentenza Scurato.

Sul piano della natura dello strumento captativo riconosciuto essere "più intrusivo delle ordinarie intercettazioni", comunque, si opera a cavallo tra "intercettazioni" (la captazione informatica è certamente anche questo) e nuova forma di mezzo di "ricerca di prova atipica", priva, però, dei requisiti della giurisdizionalità specificamente richiesti, invece, per la "prova atipica".

In questa nuova dimensione giurisprudenziale (= di *giurisprudenza creativa*) va inquadrata la critica al prodotto normativo in precedenza esaminato che si occupa, esclusivamente, delle modalità di captazione, peraltro affidate prevalentemente alla polizia giudiziaria, con evanescenti controlli e senza alcuna attenzione al momento iniziale ed allo sviluppo delle operazioni.

Una proposta commendevole, invece, deve muovere dalle previsioni dell'art. 8 Cedu, che comprende i principi del "*diritto al rispetto della vita privata*", che la nostra Costituzione racchiude nel *sistema di garanzie* di cui agli artt. 14, 15, 17, 21, 24, commi 1 e 2, 27, comma 2, e che è parte integrante ed irrinunciabile del *Preambolo penalistico della Costituzione*, per il quale nella previsione delle attività invasive dei diritti fondamentali della persona è indispensabile stabilire i presupposti autorizzativi su cui il giudice deve pronunciarsi ed i limiti entro cui è consentita l'autorizzazione, le modalità delle operazioni captative e della decifrazione dei risultati, oltre al controllo sulla effettiva sottrazione del mezzo autorizzativo. E, se quest' ultimo può essere valutato solo a posteriori attivando la sanzione di inutilizzabilità delle eventuali captazioni illecite, gli altri elementi debbono essere valutati a priori e con estremo rigore, stando la dimensione dell'invadenza nella vita privata del soggetto sottoposto al *virus* informatico, nonché al continuo controllo delle attività.

In questa prospettiva garantista l'invasività del mezzo non può prescindere: dalla presenza di un consistente *fumus* non solo del reato commesso ma anche della probabile direzione soggettiva della attività. Detto altrimenti, si palesa imprescindibile un sicuro criterio di collegamento tra l'indagine in corso e la persona da intercettare nel senso che il provvedimento autorizzativo della speciale forma intercettiva deve necessariamente dar conto delle ragioni che impongono l'intercettazione di una determina utenza che fa capo ad una specifica persona, affinché possa esserne verificata, alla luce del complessivo contenuto informativo e argomentativo del provvedimento, l'adeguatezza rispetto alla funzione di garanzia prescritta dall'art. 15, comma 2, Cost.

Da qui la necessità di contemplare, quali presupposti imprescindibili per la attivazione del peculiare strumento captativo: a) i "sufficienti indizi di colpevolezza", a mo' di elemento legittimante il provvedimento autorizzativo del giudice; b) la tassativa predeterminazione dei reati per i quali è consentito il ricorso al captatore; c) la straordinaria urgenza per il decreto autorizzativo del pubblico ministero; d) la permanenza del controllo dei risultati da parte del pubblico ministero in una alla possibilità di esercizio, in ordine allo stesso, delle relative facoltà difensive; e) il "contraddittorio" per la predisposizione del materiale da portare a conoscenza del giudice, da svolgersi in vista del riesame, se esso è impiegato per il provvedimento cautelare.

Ed allora, proiettandosi su di un possibile "articolato codicistico", quelli che seguono potrebbero essere i capisaldi dello sviluppo normativo che dovrebbe interessare il captatore informatico.

- Nessuno può utilizzare strumenti invasivi delle libertà della persona se non per espressa previsione legislativa in relazione anche al tipo ed al modo della immissione nelle libertà della persona e per atto motivato del giudice.

- È consentito l'uso di captatori informatici in dispositivi elettronici portatili o di forme telematiche satellitari per reati tassativamente individuati e nei confronti di chi è attinto da sufficienti (evidenti, chiari, provabili) indizi di colpevolezza oggetto di esplicita motivazione.

- L'impiego dello strumento in oggetto può avvenire per un periodo di tempo limitato a pena di inutilizzabilità dei risultati conseguiti oltre tale termine, a meno che non sussistono gravi indizi di colpevolezza in presenza dei quali il giudice può autorizzare la prosecuzione della attività.

- In caso di assoluta necessità ed urgenza il pubblico ministero può dare inizio alla attività i cui risultati non potranno essere utilizzati se nelle 48 ore successive non interviene provvedimento di convalida nel quale il giudice motiva sugli elementi di cui alle previsioni precedenti e sulle ragioni dell'urgenza. La violazione del termine rende inutilizzabili gli esiti delle operazioni compiute precedentemente alla convalida del provvedimento del pubblico ministero.

- Quanto alle modalità esecutive, la captazione deve svolgersi sotto la stretta osservanza dell'ufficio del pubblico ministero procedente.

- Gli esiti delle operazioni possono essere ascoltati solo dal pubblico ministero procedente al fine di estrapolare comunicazioni strettamente inerenti ai reati per i quali le stesse sono state autorizzate e debbono essere esibiti per le eventuali ulteriori richieste del pubblico ministero. In tal caso la difesa può presentare opposizione al giudice che procede per chiedere l'estromissione di atti ritenuti non inerenti al procedimento in corso o l'inclusione di comunicazioni di cui è altrimenti venuta a conoscenza.

- Siffatte attività non possono costituire notizia di reato.