FOCUS SULLE INTERCETTAZIONI TELEMATICHE

di Siro De Flammineis

Quello delle intercettazioni telematiche è un tema complesso, concretamente tecnico per i profili di innovazione tecnologica cui si àncora, ma più squisitamente giuridico perché attiene a discipline normative della vita quotidiana ed ancora colposamente inesplorate e poco approfondite. È la classica situazione di intersecazione tra scienza e diritto in cui i rapporti tra i due settori non sono dettagliatamente regolati ed è un po' lasciato agli operatori del diritto individuare la disciplina del caso concreto sulla base delle sollecitazioni tecnologiche che via via arrivano. Per questo occorre rivendicare con forza il ruolo del diritto perché l'utilizzo della scienza informatica può imprimere un grave vulnus ad alcuni diritti fondamentali della persona.
Il primo aspetto, preliminare, su cui si fonda poi tutta la disciplina in esame, **è quello relativo al conflitto di beni e valori risolto normativamente attraverso la disciplina oggi esistente**. Ebbene, ogni conflitto di valori giuridici si risolve attraverso il rinvenimento di soglie e di confini oltre i quali si determina l'illiceità dei comportamenti. Nell'ambito delle intercettazioni telematiche vengono in rilievo primariamente i valori della segretezza e della *privacy* nelle comunicazioni informatiche, ma questi valori esprimono un'esigenza di tutela in questo settore non di per sé soli ma in quanto da considerarsi secondo un significato più ampio; **poiché le comunicazioni telematiche avvengono attraverso strumenti tecnici, in giurisprudenza si è parlato dell'esistenza di un vero e proprio domicilio informatico**. L'opzione esegetica formulatrice di tale concetto è stata motivata anzitutto sulla base della ravvisata analogia delle norme penali introdotte con la l. n. 547 del 1993 e poi con la l. n. 48 del 2008 di ratifica alla Convenzione europea sul *cybercrime*, ma soprattutto con riferimento all'art. 615ter c.p., con la fattispecie della violazione di domicilio.

In questo senso ha argomentato, la Quinta Sezione della Cassazione, con la sentenza n. 37322 del 08/07/2008, Bassani, ha posto in evidenza che «*la norma in esame tutela, secondo la più accreditata dottrina, molti beni giuridici ed interessi eterogenei, quali il diritto alla riservatezza, diritti di carattere patrimoniale, come il diritto all'uso indisturbato dell'elaboratore per perseguire fini di carattere economico e produttivo, interessi pubblici rilevanti, come quelli di carattere militare, sanitario nonché quelli inerenti all'ordine pubblico ed alla sicurezza, che potrebbero essere compromessi da intrusioni o manomissioni non autorizzate. Tra i beni e gli interessi tutelati non vi è alcun dubbio [...] che particolare rilievo assume la tutela del diritto alla riservatezza e, quindi (n.d.r. specialità per specificazione), **la protezione del domicilio informatico, visto quale estensione del domicilio materiale** [...]*».
Vi è ancora da intendersi su questo punto, perché stando a queste ricostruzioni giurisprudenziali questo concetto andrebbe interpretato secondo una concezione fisica o statica, ovvero appunto quale "estensione del domicilio materiale", cioè alla stregua della disciplina del domicilio appunto fisico. La concezione fisica significherebbe: il luogo dove si trova il sistema informatico, ovvero appunto il sistema informatico stesso.

Al contrario, la concezione più adiacente ad un'interpretazione ed applicazione corretta della disciplina sulle intercettazioni telematiche sembra essere una concezione personalistica di domicilio informatico, anche più fondatamente sostenibile in considerazione della concezione personalistica che permea il nostro sistema penale alla luce dei principi costituzionali e dei diritti della personalità definiti dalla carta costituzionale tra cui appunto il diritto alla privacy e alla segretezza, ovvero, nell'ampio senso prima delineato, il domicilio informatico.

Questa prima conclusione raggiunta può essere rimarcata analizzando **un secondo aspetto di interesse** che assume un'indubbia valenza giuridica nell'ambito delle tutele penali e della disciplina processual-penalistica dell'intercettazione telematica, ovvero **il concetto di sistema informatico**; per cogliere il significato giuridico di questo ulteriore tassello occorre avere come punto di riferimento primario la definizione ampia di sistema informatico della Convenzione di Budapest .
Ebbene, questa definizione ampia è stata in qualche modo prevista dalla Cassazione, che già nel 1999 (Cass., sez. VI^, sent. n. 3067 del 4.10.1999) aveva definito quale sistema informatico una rete telefonica fissa, cioè «*un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate — per mezzo di un'attività di "codificazione" e "decodificazione" — dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, [..]*». Successivamente, le SS.UU. del 23.2.2000 (rv. 215841) **hanno ricondotto, poi, nell'alveo del sistema informatico/telematico anche un sistema telefonico mobile**.

Il principio affermato assume una particolare valenza evolutiva proprio nel riservare al giudice ogni valutazione in ordine al profilo funzionale dei sistemi informatici (e telematici) interessati, ricomprendendone ogni aspetto che sia in qualche modo legato al trattamento informatico di dati o di informazioni.
Questa visione dinamica e funzionale del concetto, entrato prepotentemente nel panorama normativo, di sistema informatico, andrebbe estesa a tutti i riferimenti concettuali che riguardano la disciplina delle intercettazioni informatiche, e così anche per il domicilio informatico; la cui definizione deve quindi prescindere dalla focalizzazione sullo strumento materiale utilizzato per trametterre le comunicazioni oggetto di intercettazione, e deve piuttosto attenere a tutti i luoghi dove una persona fa uso di un sistema informatico, ovvero svolge un trattamento informatico di dati o informazioni che esplica un esercizio della libertà fondamentale di ciascuna persona di comunicare segretamente.

Analoghe considerazioni devono essere svolte con riguardo ad un altro concetto giuridico che viene in rilievo, forse sottovalutato nella dialettica processuale, quello di **prova informatica**: ormai entrata a pieno titolo nel sistema penale.
Secondo una certa impostazione giurisprudenziale la prova informatica ricadrebbe nell'ambito delle c.d. prove atipiche.

In questo senso la Cassazione è intervenuta nel 2010 Cass., sez. V, 14 ottobre 2009, Virruso e altri, in CED Cass., n. 246954, (vedi dopo) escludendo la lesione di diritti fondamentali ed annoverando l'atto dell'inserimento di *virus* informatici idonei a captare tutti i dati che vengono inseriti all'interno di un *personal computer* tra i mezzi atipici di ricerca della prova; si è esclusa l'applicabilità delle norme di cui agli art. 266 c.p.p. e ss. con riferimento alla mera captazione di dati preesistenti su un *computer* e distinguendo appunto tra dati informatici preesistenti e flusso di comunicazioni. Non può esser sottovalutato che i *files* allocati su un *hard disk*, infatti, integrano una mera potenzialità rappresentativa che – seppur definita nei suoi contorni – prende forma ed esistenza effettiva, divenendo "rappresentazione" solo mediante complesse operazioni. Le quali operazioni, si ribadisce, lungi dal consistere in una mera "lettura" del dato, lo elaborano, modificandone lo stato fisico.

Per queste ragioni in dottrina si ritiene preferibile considerare ricompresa nel novero delle prove atipiche la prova consistente nell'esame del contenuto informativo presente in formato digitale nell'*hard disk* di un *computer*, mediante sua estrapolazione a mezzo di apposite operazioni di carattere informatico. Ma se il metodo di acquisizione di questa prova è disciplinato espressamente dalla legge non sarà più una prova atipica ma tipica o tipizzata, intanto in dottrina si parla di prova informatica come prova atipica in quanto ci si riferisce a strumenti di acquisizione atipici, della stessa prova nel corso delle indagini, ma se lo strumento di ricerca della prova è tipico allora lo sarà anche la prova, e allora qual è la prova tipica che si acquisisce mediante intercettazione? **Se ci riferiamo in modo più specifico al campo delle intercettazioni telematiche ci rendiamo conto che il concetto di prova informatica e telematica tipica oggetto del mezzo di ricerca delle intercettazioni deve essere ancora definito e necessariamente inteso in senso più ampio di quanto finora considerato in giurisprudenza**. Oggetto di intercettazione, infatti, sono tutti i *files* potenzialmente rappresentabili all'interno del documento cartaceo e del *monitor*.

Con riguardo alle forme di captazione la Cass. nel 2010, c.d. sentenza Virruso, ha affermato che: «[...] *è legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel "personal computer" in uso all'imputato e installato presso un ufficio pubblico, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati. (Nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'"hard disk" del computer in uso all'imputato, aveva avuto ad oggetto non un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elettronico", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen.)*». **Tuttavia questa sentenza determina una grande confusione perché ritiene necessariamente ricompresi nell'ambito del 266 c.p.p. esclusivamente i flussi di comunicazioni richiedente un dialogo con altri soggetti: ma l'art. 266, co.1, non dice affatto questo, parla di "altre forme di telecomunicazione"**.
La prova tipica oggetto di intercettazione è la comunicazione, nel senso del passaggio di dati da un mittente a un destinatario, il flusso è uno scambio di dati numerici (*bit*) e oggetto dell'intercettazione è la connessione tra *computer*: si prescinde dal contenuto dei dati, che può essere nella forma del dialogo tra soggetti quindi una conversazione ovvero anche nella forma del monologo, cioè di messaggi senza richiesta di risposta, di un video senza audio, cioè contenuti non strettamente comunicativi secondo il dettato della giurisprudenza finora maggioritaria in ordine all'oggetto legittimo dell'attività di intercettazione.
Se, invece, il dettato giurisprudenziale quando parla di dialogo tra soggetti intende tra sistemi informatici e non persone fisiche allora si può essere parzialmente d'accordo perché comunque ci possono essere delle ipotesi in cui alcuni dati vengono immagazzinati inizialmente sul computer per poi essere proiettati tramite *software* all'interno di un sistema operativo che li trasmette e li comunica, in tempi successivi rispetto all'elaborazione interna.

In effetti, un aspetto oggi sostanzialmente privo di adeguata "copertura" legislativa, riguarda l'acquisizione di *email* che siano state già trasmesse (al pari di quanto avviene per gli SMS), e che si trovino memorizzate presso il *server* del gestore del servizio perché, ad esempio, non ancora scaricate dal destinatario. Ed infatti, se non vi è dubbio che la trasmissione di *email* si sostanzia in una comunicazione telematica di flussi informatici, come tale soggetta alla disciplina delle intercettazioni telematiche, è possibile rilevare come tali operazioni dovrebbero riguardare solamente l'attività di captazione di comunicazioni contestuali: sicché non dovrebbe rientrare in tale categoria l'attività di acquisizione di dati informatici oggetto di comunicazioni non contestuali perché già avvenute.
Ma non è così: il concetto di comunicazione contestuale è restrittivo e non tiene adeguatamente in conto l'espansione tecnologica. Poiché l'*email* è un servizio che non necessita di connessione attiva, cioè gli utenti non devono essere fisicamente in rete al momento del trasferimento dei dati perché è il *mail server* che immagazzina i dati e li trasferisce, allora le *email* non sarebbero oggetto di intercettazione? Allora bisogna dire che l'*email* già inviate e pervenute al destinatario e archiviate da lui non possono essere oggetto di intercettazione perché non sono più comunicazione, sono assimilabili al concetto di corrispondenza; se invece ci sono *email* archiviate nella cartella bozze in un *account* accessibile anche da altro utente, anche se non è una *email* inoltrata al destinatario è possibile l'intercettazione del secondo utente al momento dell'accesso alla casella della bozza, è anche questa una comunicazione anche se è l'*email* non è inviata.

E poi SKYPE: poiché l'unico modo di intercettare skype che usa forme di criptazione dei dati non pubbliche e non conosciute è utilizzare un trojan o un worm, questo deve essere fatto prima che il dato, la comunicazione entri nella rete skype, trasferendo la conversazione in un'altra stazione ricevente senza lasciare tracce, allora questa non è una comunicazione perché non si è formato il dialogo? Una risposta di questo tipo non sarebbe conforme all'evoluzione tecnologica. ©