DIGITAL EVIDENCE E INTERCETTAZIONI TELEMATICHE

di Sergio Barbiera e Damiano Galati

Il rapido ed incessante progresso della tecnologia telematica ed il sempre più accresciuto bisogno di "*right to privacy*", ormai fortemente compromesso dai *social networks* incuranti del numero di Dunbar[(1)], richiedono l'adozione di strumenti investigativi idonei ad accertare i fatti di reato di maggior allarme sociale. La sempre più diffusa anonimizzazione delle comunicazioni e conversazioni telematiche richiede il ricorso a strumenti investigativi intrusivi idonei a raccogliere il dato informatico contenuto nell'host (*one time copy*) ovvero a captare il flusso continuo (*on line surveillance*) della navigazione o della conversazione (cd. "pedinamento virtuale"). **Risulta quindi d'uopo, anzitutto, analizzare sotto quale paradigma normativo sussumere lo strumento investigativo *de quo*, in mancanza di una specifica disciplina giuridica ed alla luce del principio statuito dall'art. 189 c.p.p.**

Prima di operare il ragionamento giuridico-investigativo inferenziale, occorre analizzare le modalità tecniche della captazione info-telematica con la quale, di fatto, l'organo investigativo acquisisce il contenuto della memoria di un dispositivo informatico (compresi i dati della navigazione, cd. "intercettazione telematica passiva" o "*sniffing*") ovvero traccia e capta i dati comunicativi in tempo reale: attività, entrambe, che, nel caso che interessa, vengono eseguite con legittime intrusioni "da remoto" attraverso l'immissione nel sistema del *client* di un apposito programma (*trojan*, *sniffer*, *backdoor et similia*).

Orbene, volendo operare un parallelismo con gli ordinari strumenti di ricerca della prova tipizzati, è possibile, nel caso di specie, operare il richiamo alla disciplina dettata per la perquisizione e le intercettazioni ambientali. Allorché, infatti, l'*online search* sia esclusivamente finalizzata ad acquisire il contenuto dell'unità di memoria dell'*host* (da remoto) - *sniffing* - la disciplina applicabile sarebbe quella prevista dall'art. 247 codice di rito con le conseguenti attività apprensive *ex* art. 253. **Sicchè la perquisizione elettronica (ed il conseguente eventuale sequestro), prevedendo la convalida da parte dell'A.G., innesca il meccanismo di garanzia defensionale di conoscibilità da parte dell'indagato, così vanificando la proficua prosecuzione dell'indagine**: in tal caso il P.M. potrebbe ritardare ex art. 366 il deposito degli atti per un breve lasso temporale (30 gg) sovente incompatibile con la durata delle indagini, ovvero, alternativamente, la polizia giudiziaria procedente potrebbe ritardare od omettere gli atti di propria competenza, laddove si verta nelle ipotesi tassativamente indicate dall'art. 9 /6 L. 146/2006 come modificato dall'art. 8 L. 136/2006, lasciando pertanto impregiudicata la proficua prosecuzione delle preliminari investigazioni.

Tuttavia, nella ordinaria prassi investigativa, **per determinate particolari fattispecie delittuose, risulta d'uopo attivare una sorta di "pedinamento elettronico" attraverso il monitoraggio continuo e costante della navigazione ovvero della corrispondenza informatica**: in tal caso, a prescindere dal ricorso, ove possibile, alle modalità operative giudiziarie mutuate dalla vigente legislazione *undercover ut supra*, non pare condivisibile quella dottrina che la ritiene assimilabile ad una "perquisizione continua" (con "ricerca della *res* non selettiva") che termina solo con la chiusura delle indagini. In tal caso appare più correttamente applicabile "per analogia" la disciplina delle intercettazioni ambientali, atteso che la pervicace invasività dello strumento nella *privacy* del soggetto controllato deve superare un vaglio giurisdizionale *super partes* ed operare pertanto solo *officio iudicis*, seppur, *de jure condendo*, **sarebbe auspicabile l'adozione di una nuova normativa che disciplini organicamente e dettagliatamente la materia dei mezzi di ricerca della prova al passo con le nuove tecnologie comunicative**.

Allorché, invece, debba eseguirsi una intercettazione telematica attiva nell'*host* del *client* da remoto la sistematica del codice di rito, seppur non su un piano definitorio, sembra richiamare il *common core* della disciplina dettata per le cd. "intercettazioni ambientali", soprattutto nelle ipotesi in cui si cerchi di captare, non solo il contatto tra sistemi informatici, ma, vieppiù, lo scambio di contatti tra utenti a sfondo comunicativo (ad *exemplum tantum*, le conversazioni tramite Skype o What's up). In tal caso, come il provvedimento autorizzativo delle intercettazioni ambientali contiene *ex* sé l'"autorizzazione legale" alla violazione del domicilio per la collocazione della microspia nel sito da ambientalizzare, così il provvedimento autorizzativo della captazione telematica contiene implicitamente il "nulla osta" all'esecuzione delle operazioni che può solo avvenire attraverso la "inoculazione" nel sistema da monitorare dello *spyware* idoneo.

Altro e diverse problema, da ultimo, attiene all'autenticità e immutabilità del dato ricavato: *nulla quaestio* per ciò che attiene al dato fonetico-vocale, sempre suscettibile di esame tecnico-comparativo; il dato documentale, invece, suscettibile di possibili artefazioni, dovrebbe essere certificato dal titolare del *provider* custode dei dati, conformemente alla disciplina sancita nel codice sulla *privacy*.

Quanto al valore giuridico del dato info-telematico ricavato, ad esso si applicano pacificamente i canoni ermeneutici consolidati sul valore probatorio dei documenti e delle intercettazioni. ©

NOTE

1. Il numero di Dunbar è un limite cognitivo teorico che concerne il numero di persone con cui un individuo è in grado di mantenere relazioni sociali stabili, ossia relazioni nelle quali un individuo conosce l'identità di ciascuna persona e come queste persone si relazionano con ognuna delle altre. Rif. Malcolm Gladwell, *The Tipping Point - How Little Things Make a Big Difference*, Little, Brown and Company, 2000. ◊