UN NUOVO STRUMENTO PER LE INDAGINI PENALI: IL CAPTATORE INFORMATICO

A CURA DEL DOTT. COSIMO CAPUTO

Adottato da ormai più di un decennio nelle indagini penali, il captatore informatico è ancora posto sotto la lente di ingrandimento degli operatori del diritto, i quali, con atteggiamento in parte incuriosito e in parte diffidente, sono alla ricerca di un punto di equilibrio tra le esigenze di accertamento che ne suggeriscono l'utilizzo e le garanzie della persona, suscettibili di essere compresse da un mezzo di ricerca della prova che ha capacità straordinariamente invasive.

L'evoluzione tecnologica ha richiesto un adeguamento delle metodologie di investigazione adoperate dagli organi inquirenti, basti pensare al fatto che oggi la comunicazione avviene prevalentemente attraverso applicazioni di messaggistica istantanea, quali ad esempio Whatsapp, Messenger e Telegram, che, caratterizzate da forme di crittografia end to end, impediscono di apprendere la conversazione con le modalità proprie dell'intercettazione delle e-mail, la cui acquisizione avviene mediante la mera duplicazione della casella di posta elettronica del soggetto monitorato. Ecco che, per superare tale ostacolo, si rende indispensabile accedere all'interno dell'apparecchio elettronico, così da avere conoscenza di ciò che viene digitato sulla tastiera e visualizzato sullo schermo.

La legge 48/2008 di "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica*" ha offerto una sistemazione organica all'attività di ricerca della prova informatica, ponendo una prima soluzione ai problemi della *chain of custody* del dato informatico.

Nell'era in cui "*data is the raw material of the information age*", la filiera del dato diventa bene essenziale da proteggere non solo come asset aziendale ma anche in sede processuale, quando la *chain of custody* diventa requisito indispensabile per assicurare la tracciabilità del dato informatico e la sua piena utilizzabilità in sede dibattimentale.

La Convenzione di Budapest sul *cybercrime* ha tentato di bilanciare le garanzie processuali del diritto alla difesa e la tutela della purezza del dato informatico, cercando di salvaguardarne l'utilizzabilità a fronte dell'ontologica fragilità, alterabilità e falsificabilità del dato informatico.

Il complesso di norme codificate nella l. 48/2008 disciplina le indagini concernenti sistemi o programmi informatici e telematici, attingendo ai modelli legali tipici di formazione della prova, quali le ispezioni, le perquisizioni, i sequestri e gli accertamenti irripetibili.

Ecco, quindi, che quando si parla di *digital evidence*, come quelle operazioni di investigazione informatica, vengono in rilievo l'art. 187 c.p.p. sull'oggetto della prova, l'art. 189 c.p.p. sulle prove non disciplinate dalla legge, l'art. 192 sulla valutazione della prova e degli indizi, l'art. 254 bis c.p.p. in tema di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazione, l'art. 352 co.1-bis c.p.p. avente ad oggetto la perquisizione ad iniziativa della polizia giudiziaria di sistemi informatici o telematici, l'art. 360 c.p.p. sugli accertamenti tecnici irripetibili.

La prova digitale ha natura impalpabile, immateriale e volatile e il più delle volte irripetibile. Estremamente facile da modificare, alterare o danneggiare, errori nell'acquisizione, nella conservazione, nella *chain of custody* e quindi della conformità della copia all'originale potrebbero comportare l'adulterazione del vaglio giudiziale.

La prova tecnologica scientifica ha natura indiziaria. Trova applicazione il paradigma tipico del ragionamento inferenziale e l'efficacia dimostrativa dell'apporto sarà nulla ove non corredato da precisione, univocità e concordanza.

La normativa in esame, dando esecuzione alla Convenzione di Budapest, ha stabilito che le indagini vengano svolte mediante l'ausilio del consueto armamentario dei modelli legali tipici di formazione della prova. Tuttavia, in almeno due ipotesi lo schema di recupero dei modelli classici non risulta applicabile. Si fa riferimento all'infiltrazione in un sistema informatico ed alla localizzazione o pedinamento satellitare, solo convenzionalmente qualificabile come intercettazione ex art. 267 c.p.p., casi in cui i mezzi tipici di ricerca della prova mal si attagliano all'indagine informatica effettivamente posta in essere.

Con il termine infiltrazione in un sistema informatico si intendono quelle operazioni finalizzate all'installazione di software di tipo trojan capace di generare un prodotto probatorio, facilmente qualificabile in termini di perquisizione irripetibile e quindi da inserire nel fascicolo per il dibattimento ai sensi dell'art. 431 lett. b. c.p.p.

La riconduzione a fattispecie tipica di mezzo di ricerca della prova spesso finisce per essere una forzatura e pertanto occorre far ricorso all'art. 189 c.p.p., al fine di inquadrare tali strumenti investigativi nell'alveo dei mezzi di ricerca atipici.

Tali nuove opportunità di indagine hanno avuto ulteriore spazio con la più recente normativa (D.Lgs. n. 216 del 2017, L. n. 3 del 2019, D.l. n. 161 del 2019) che, con riferimento al sistema delle intercettazioni, ha ampliato i fenomeni criminali per i quali si ritiene opportuno una maggiore libertà di azione degli inquirenti, anche mediante accesso ai dispositivi informatici: ora, anche per i più gravi delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione sono applicabili le disposizioni in passato limitate ai soli procedimenti per criminalità organizzata e terrorismo.

Ciò significa che, per questi reati, oltre ad essere semplificate le condizioni per procedere alle già invasive intercettazioni, le operazioni di ascolto possono essere effettuate anche nel domicilio del soggetto intercettato con il captatore informatico.

Il potere di disporre le intercettazioni mediante captatore informatico è attribuito in via ordinaria al giudice per le indagini preliminari che provvede su richiesta del p.m. Il legislatore, tuttavia, accanto alla procedura ordinaria ha previsto la possibilità di attivazione officiosa da parte del titolare delle indagini nei casi in cui sussistano ragioni di urgenza tali da rendere indifferibile l'inizio delle operazioni captative.

L'art. 267, comma 2 bis, c.p.p., contiene una disciplina speciale per il ricorso in via d'urgenza al trojan virus e prevede che il pubblico ministero, può disporre l'immediato inizio delle operazioni con decreto motivato. La validità dell'iniziativa officiosa è condizionata alla successiva tempestiva convalida da parte del giudice per le indagini preliminari, in mancanza della quale è stabilita l'inutilizzabilità dei risultati eventualmente acquisiti. La riforma "Bonafede" in materia di intercettazioni – d.l. n. 161 del 2019, convertito con modificazioni dalla l. n. 7 del 2020 – è intervenuta anche sul procedimento d'urgenza del pubblico ministero, ampliandone ulteriormente il raggio operativo.

Per effetto della novella sono, ora, ricompresi tra i reati per i quali è possibile l'attivazione officiosa del p.m., in aggiunta alle fattispecie di cui all'art. 51, co. 3 bis e 3 quater c.p.p., i procedimenti per i delitti contro la p.a. commessi dai pubblici ufficiali o dagli incaricati di pubblico servizio per i quali sia prevista una pena edittale non inferiore nel massimo a 5 anni. Sotto il profilo in esame, il legislatore sembra aver dato seguito al disegno inaugurato dalla l. n. 3 del 2019, c.d. "*spazza-corrotti*", mosso dall'intento di realizzare una progressiva assimilazione, anche per quanto riguarda gli strumenti investigativi, dei più gravi reati contro la pubblica amministrazione alle ipotesi delittuose di terrorismo e di criminalità organizzata.

Restano esclusi dall'operatività del co 2 bis dell'art. 267 c.p.p., tutti i procedimenti relativi alle fattispecie di cui all'art. 266, comma 1, c.p.p., in relazione ai quali il ricorso in via d'urgenza al captatore informatico non è, *de lege lata*, consentito. Nei procedimenti per i reati "*comuni*", pertanto, l'attivazione della cimice informatica dovrà, necessariamente, seguire l'iter ordinario costituito dalla richiesta del p.m. e dall'emissione del decreto autorizzativo da parte del giudice. La scelta del legislatore, forse dettata da una generale sfiducia nei confronti del nuovo mezzo di ricerca della prova, risulta priva di solide fondamenta. Deve riconoscersi, infatti, che la ratio sottostante al ricorso d'urgenza allo strumento captativo, non è legata a valutazioni di politica criminale, bensì risponde esclusivamente a concrete esigenze investigative che, se sorrette da circostanziate motivazioni e non distorte nella prassi, risultano senz'altro meritevoli di tutela indipendentemente dal titolo di reato per il quale si procede.

Per quanto attiene ai presupposti del decreto d'urgenza, l'art. 267, comma 2 bis c.p.p., compie un rinvio alla disciplina contenuta al comma 2, stesso articolo. La disposizione richiamata chiarisce che il periculum in mora, fulcro del potere officioso, deve ritenersi integrato quando «*dal ritardo possa derivare grave pregiudizio alle indagini*», ossia quando sussista un rischio concreto che l'efficacia dell'atto investigativo, se non eseguito in tempi ravvicinati, verrebbe irrimediabilmente pregiudicata. Con riferimento al captatore informatico, il legislatore ha inteso enfatizzare l'obbligo del pubblico ministero di motivare, nella richiesta di convalida del decreto, le ragioni di urgenza. Il comma 2 bis dell'art. 267 c.p.p. stabilisce, infatti, che il decreto deve specificamente indicare «*le ragioni di urgenza che rendono impossibile attendere il provvedimento del giudice*».

Gli ulteriori presupposti di legge del procedimento d'urgenza si ricavano, poi, implicitamente dalla disciplina generale del captatore tracciata dal combinato disposto degli artt. 266 e 267 c.p.p. In primo luogo, anche il decreto emesso dal pubblico ministero, al pari di quanto previsto per il provvedimento autorizzativo del giudice, deve indicare, indipendentemente dalla fattispecie di reato per la quale si procede, le «*ragioni che rendono necessaria tale modalità di svolgimento delle indagini*».

Nell'adottare il decreto, il titolare delle indagini sarà ugualmente tenuto, quanto meno, a prospettare una ragionevole infruttuosità degli altri, diversi e meno invasivi, mezzi di ricerca della prova e un più alto rischio di insuccesso delle operazioni tradizionali.

Per i gravi delitti contro la pubblica amministrazione, l'ultimo intervento legislativo ha apportato significative modifiche sotto due concorrenti profili. In prima battuta, il d.l. n. 161 del 2019, interpolando il comma 1 dell'art. 267 c.p.p, ha eliminato l'obbligo per il decreto autorizzativo di fissare anticipatamente i luoghi e il tempo in cui è consentita l'attivazione del microfono. In sede di conversione del decreto-legge, poi, il legislatore ha previsto uno sforzo motivazionale aggravato per l'autorità procedente nei casi di intercettazioni infra-domiciliari disposte nei procedimenti per i delitti contro la P.A. L'art. 266, co. 2-bis, c.p.p., prevede ora che, nei casi in esame, il decreto autorizzativo debba indicare le ragioni che suggeriscono l'utilità del ricorso al mezzo investigativo all'interno dei luoghi di privata dimora.

Pur nel silenzio dell'art. 267, co. 2-bis, c.p.p., ragioni di coerenza interna alla disciplina in esame inducono a ritenere che il predetto onere motivazionale operi, non soltanto per il provvedimento autorizzativo del giudice, ma anche per il decreto con il quale il pubblico ministero dispone d'urgenza l'avvio delle operazioni captative. L'aggravamento opera soltanto sul piano motivazionale e non come presupposto di ammissibilità del mezzo di ricerca della prova: anche dopo l'ultimo intervento normativo, infatti, i più gravi reati contro la pubblica amministrazione restano assimilati, quanto a presupposti e limiti applicativi, ai reati di criminalità organizzata non comune. Il proposito del legislatore di trovare un più mirato equilibrio tra le esigenze investigative e la tutela del domicilio, perseguito attraverso l'interpolazione dell'art. 266, co. 2-bis, c.p.p., rischia pertanto di rimanere deluso o, comunque, rimesso alla più ampia discrezionalità dell'autorità giudiziaria.

Il comma 3 dell'art. 267 c.p.p., stabilisce che nel decreto d'urgenza siano indicate le modalità e la durata delle operazioni. Il provvedimento del pubblico ministero ha, per l'appunto, l'effetto di autorizzare la polizia giudiziaria a dare immediato corso alle operazioni di inoculamento e attivazione del trojan sul dispositivo-bersaglio.

Per quanto riguarda la durata delle operazioni captative a mezzo captatore, trova applicazione la disciplina derogatoria contenuta nell'art. 13, comma 2, d.l. n. 152 del 1991, che stabilisce il termine lungo di 40 giorni, con possibilità di successive proroghe di 20 in caso di permanenza dei presupposti richiesti *ab origine*.

Infine, trovano applicazione le ordinarie regole procedurali che impongono al pubblico ministero, dopo aver adottato il decreto d'urgenza, di comunicarlo immediatamente – e, comunque, entro il termine di 24 ore – al giudice per le indagini preliminari. La convalida del GIP deve intervenire, a pena di inutilizzabilità assoluta dei risultati acquisiti, entro il termine perentorio di 48 ore dall'emissione del decreto. Le conversazioni registrate sulla base di un decreto d'urgenza non tempestivamente convalidato devono, infatti, considerarsi *tamquam non esset* e ne è vietato qualsiasi utilizzo.

Per quello che riguarda le disposizioni di ordinamento processuale concernenti la documentazione delle attività captative a mezzo trojan virus, deve osservarsi che la disciplina in oggetto si ricava in modo non del tutto perspicuo dal combinato disposto degli artt. 268 c.p.p e 89 disp. att. c.p.p. La norma cardine resta l'art. 268 c.p.p, il cui comma 1 pone l'obbligo generale di verbalizzazione delle operazioni, dovendo intendersi come tale l'attività di documentazione per iscritto degli adempimenti affidati alla polizia giudiziaria, a partire dall'inoculazione del virus fino alla sua definitiva disinstallazione dal dispositivo.

Quanto al contenuto del verbale, agli elementi indefettibili in comune alle ipotesi di intercettazioni "tradizionali" – quali gli estremi del decreto di autorizzazione, la descrizione delle modalità di registrazione, l'annotazione del giorno e dell'ora di inizio e fine dell'intercettazione, i nominativi di chi ha preso parte alle operazioni – se ne aggiungono altri specifici per l'uso del trojan virus. In questi casi, l'art. 89, comma 1, disp. att. c.p.p, stabilisce che nel verbale vengano, altresì, riportati l'indicazione del programma informatico utilizzato e, "*ove possibile*", i luoghi di attivazione del microfono del dispositivo.

L'identificazione esatta del luogo di attivazione della "*cimice ambientale*" riveste una particolare importanza nei procedimenti per reati "*comuni*" di cui all'art. 266, comma 1, c.p.p., in relazione ai quali il decreto autorizzativo deve preventivamente indicare, anche indirettamente, gli ambiti spaziali nei quali è consentita l'attivazione del microfono del dispositivo mobile infettato. La prescrizione risulta consolidata dal raccordo con le disposizioni dei commi 1 bis e 3 dell'art. 271 c.p.p., in forza delle quali i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto di autorizzazione sono affetti da inutilizzabilità processuale assoluta e il giudice è tenuto, in ogni stato e grado, a disporne la distruzione, salvo si tratti del corpo del reato.

Così tratteggiati i profili operativi del *trojan virus*, deve valutarsi positivamente lo sforzo del legislatore teso a delineare una disciplina di dettaglio che, sulla base dell'esperienza maturata sul campo dalle procure, metta a fuoco alcune delle problematiche operative di maggior momento. Se è vero, infatti, che il captatore informatico rappresenta nel panorama processuale attuale lo strumento di indagine con il più elevato tasso tecnologico e dalle più alte potenzialità accertative, ci si deve aspettare che il delicato equilibrio degli interessi in gioco si misurerà dall'adozione di più o meno efficaci garanzie tecniche.

Il livello di affidabilità dei programmi informatici utilizzati per l'esecuzione delle intercettazioni, la trasparenza dell'agire delle società incaricate delle operazioni, la tutela dell'integrità dei dati acquisiti e

la loro successiva conservazione, sono solo alcune delle questioni destinate a travalicare la dimensione strettamente operativa del captatore per divenire punti nodali intorno ai quali, sembra di poter concludere, si giocherà la tenuta costituzionale del nuovo metodo di accertamento processuale.