POSTFAZIONE

di Stefano Elli, giornalista
Il Sole 24 Ore

Due cose sono certe. La prima: la prova digitale non si trova con il luminol. La seconda: la pistola fumante sul web si sposta a velocità C (che poi sarebbe quella della luce). La prova digitale, però, al pari delle cosiddette prove biologiche, va raccolta, isolata e protetta, analizzata sotto gli aspetti dell'ammissibilità in giudizio e infine prodotta in dibattimento. Una prova biologica raccolta correttamente, ma trattata in modo maldestro, rischia di essere contaminata e di diventare inutilizzabile. Lo stesso dicasi (o dovrebbe dirsi) per una prova digitale. Dalla raccolta della prova, che può essere effettuata attraverso vari tools investigativi (perquisizioni informatiche, trojan, etc.), si passa alla fase successiva: la sua messa in sicurezza. In questo caso proteggerla significa isolarla e renderla asettica, in qualche modo inattaccabile, da elementi esterni che potrebbero agevolmente corromperla. Ecco perché la fase della blindatura della digital evidence rappresenta forse quella più importante.

Dalla cronaca ci arrivano storie e vicende affascinanti. L'operazione Trojan shield del 2018, frutto dell'idea degli uomini dell'FBI, che approfittarono della chiusura di una piattaforma per comunicazioni criptate più utilizzata dalle mafie chiamata Phantom. I Gmen del Bureau si chiesero: perché sprecare risorse ed energie per inseguire le varie piattaforme presenti sul mercato clandestino? Creiamone piuttosto una direttamente noi e imponiamola sul mercato. Nacque così la piattaforma Anom, nome assai evocativo, astutamente scelto dal Bureau. La fecero nascere in Australia (territorio apparentemente neutrale sotto il profilo del contrasto alla criminalità organizzata) e da qui si diffuse, attraverso la Turchia, ben presto

accreditandosi tra vari gruppi criminali come una delle piattaforme più inattaccabili del mondo digitale. Peccato (o meglio per fortuna) che fosse gestita da Quantico. Trojan Shield portò ad alcuni risultati di notevole rilievo. L'8 giugno 2021 si decise di chiudere le porte della "tonnara". Risultato: 800 arresti di appartenenti ad almeno 300 consorterie criminali di un centinaio di nazioni. Otto tonnellate di cocaina sequestrata, 22 di marijuana, due tonnellate di droghe sintetiche, 250 armi da fuoco. Anni prima, sempre l'FBI, aveva effettuato un'operazione analoga: infiltrò un suo uomo in una banca sita alle isole Grenadines: la the New Bank Limited, guidata da italiani, sospettata di riciclare centinaia di milioni di dollari. Il falso impiegato si mise al lavoro e, anni dopo, la banca venne chiusa con un'operazione militare in grande stile. La differenza tra le due operazioni è chiara: la prima è stata condotta attraverso l'uso del cosiddetto TechInt, la seconda con tecniche di HumInt. Una terza operazione coordinata dalla Polizia Postale Italiana, battezzata Luna Park, si è avvalsa di tecniche miste HumInt-TechInt, infiltrando agenti in rete che fingendosi "clienti" misero in atto una delle più significative operazioni contro la pedopornografia mai eseguite in Europa.

Detta così sembra semplice: non lo è affatto.

La transnazionalità della rete, l'uso diffuso della crittografia e la necessità di armonizzare diverse giurisdizioni sul tema dell'ammissibilità delle prove pongono sovente problemi assai seri. La sensibilità dei vari impianti legislativi internazionali a temi come la privacy, la protezione sociale e la sicurezza non è sempre la stessa e spesso pone ostacoli di rilievo. Così come il trattamento delle varie fasi delle intercettazioni e del loro "prodotto", siano esse ambientali, telefoniche o captate attraverso trojan inoculati all'interno di server o di smartphone.

Come si vede, il mare dei contenuti sull'uso processuale della digital evidence, e delle ulteriori ricadute derivanti dall'implementazione dell'intelligenza artificiale, è vasto e poco

navigato.

Mancava una guida sistematica, ragionata, argomentata, che spaziasse dalla dottrina alla giurisprudenza, sino alla normativa in vigore, un manuale d'uso che spiegasse lo stato di un'arte complicatissima non solo attraverso casi documentati, ma pure attraverso un approccio tecnico e scientifico rigoroso sulla digital forensics e con riflessioni filosofiche e approfondimenti concettuali sulla formazione della prova.

Ora c'è.