Digital Forensics - Come si evolve la legge contro i reati informatici

Date : 29 settembre 2016

La digital forensics è ormai una disciplina di un certo peso e nota al pubblico grazie ad eventi – purtroppo spesso spiacevoli – che hanno visto come protagonisti consulenti tecnici e legali impegnati a estrarre e validare prove digitali da computer, cellulari, scatole nere, web, cloud o qualunque possibile fonte d'informazione elettronica.

Dagli omicidi ai furti d'identità, dai dipendenti infedeli allo stalking, dalle rapine all'accesso abusivo nei sistemi informatici: non si contano i reati per i quali si dimostra necessario, insieme alle attività tradizionali, un esame di qualche evidenza digitale. Esame che sempre più spesso viene eseguito da tecnici professionisti e validato da giuristi in grado di comprendere le dinamiche e le difficoltà che gravitano intorno a un mondo di prove "volatili" spesso non correttamente interpretato con i criteri tradizionali.

Il settore è così ampio e variegato che spesso chi non avrebbe mai immaginato di dover prima o poi ricorrere alla digital forensics si ritrova a cercare consulenza nel momento del bisogno riducendosi talvolta a pensare di poter sostituire il tecnico professionista oppure – peggio ancora – affidandosi a periti forensi improvvisati che fino al giorno prima assemblavano computer per la vendita al dettaglio (senza nulla togliere a chi per lavoro assembla computer).

Per quanto oggi la digital forensics risulti una disciplina piuttosto consolidata, giova ricordare che fino al 2008 la Legge italiana aveva pochi riferimenti che contemplassero i reati informatici o le modalità di acquisizione della prova digitale, che spesso veniva realizzata con copia/incolla di file o strumenti inadeguati.

La Giustizia ha fatto enormi passi avanti proprio nel 2008, con la Legge 48, che ha recepito la Convenzione di Budapest sui reati informatici resa dal Consiglio d'Europa nel 2001. Sono stati così modificati alcuni articoli del Codice Penale aggiungendo importanti precisazioni sulle modalità di acquisizione, trattamento e conservazione della prova digitale.

Una delle integrazioni più rilevanti riguarda proprio l'acquisizione della prova, che deve essere eseguita "adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione", specificando che la copia deve essere realizzata "con una

procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità”. Su questa base, negli ultimi anni si è costruita la disciplina della digital forensics, che si divide poi nelle branchie della computer, mobile, audio, video e network forensics per arrivare alla bitcoin forensics che riguarda le attività d’indagine sulle criptovalute.

Il mondo delle perizie forensi è in rapida espansione, così come sono in aumento gli strumenti a disposizione dei tecnici che devono essere in grado di scegliere e utilizzare quelli che maggiormente si addicono al caso in analisi.

Si pensi a quante volte, ad esempio, le aziende si trovano di fronte a decisioni circa il possibile esame di attrezzatura aziendale in dotazione a dipendenti o ex dipendenti che si sono rilevati essere “infedeli” per aver acquisito dati riservati da utilizzare poi nella loro nuova posizione lavorativa. Allo stesso modo, non si contano i fascicoli ove gli avvocati hanno sottovalutato la fase della perizia informatica trovandosi poi di fronte a prove non utilizzabili o persino non trovando delle prove che erano presenti prima dell’attività d’indagine.

Articolo a cura di: **Paolo Dal Checco**