

Prefazione

Sì, il mondo sta cambiando. Questo è vero in generale, ovviamente, ma lo si nota anche nel piccolo e speciale ecosistema costituito dalle discipline forensi. Certo non lo si sente nella terra e nell'acqua, come memorabilmente diceva Fangorn (no, non Galadriel: andate a rilegervi il libro!) ma basta accendere la televisione dopo cena per accorgersene. Infatti, scemato ormai il successo dei *Grandi Fratelli* e delle *Isole dei Famosi*, e cavalcando invece l'onda dei vari *CSI* d'oltreoceano e relativi surrogati nostrani, i morbosi interessi catodici del grande pubblico sono adesso sempre più appagati da innumerevoli trasmissioni che fanno delle pagine di cronaca, soprattutto quella nera, il più attraente dei reality. Proliferano così non solo fiction incentrate su poco credibili investigatori scientifici di questa o quella forza di polizia, ma soprattutto programmi di scarso approfondimento basati sulla presenza in studio di improbabili esperti e avvocati *showmen* che, con l'accondiscendente complicità di conduttori spesso più imbarazzanti che imbarazzati, discettano tuttologicamente sull'ultimo caso di efferato omicidio o sequestro di persona in una sorta di tribunale virtuale, parallelo a quello reale ma mediaticamente assai più accattivante. Sembra dunque che gli italiani, oltre a essere da sempre valenti commissari tecnici della nazionale e perfetti presidenti del Consiglio, da qualche tempo a questa parte si siano anche scoperti tutti esperti criminologi. E così discipline in precedenza oscure ed emarginate come l'anatomopatologia o la balistica sono divenute da un giorno all'altro conoscenze di uso quotidiano, mentre le tecniche di *profiling* sono ormai oggetto di discussione da bar e il codice di procedura penale è assurdo ad amena lettura da comodino delle casalinghe non solo di Voghera.

Un effetto positivo di questa piccola grande rivoluzione nei costumi televisivi nazionali è stato quello di aver contribuito a diffondere estesamente la conoscenza dei principi e delle tecniche di investigazione scientifica, che oggi giorno costituiscono un supporto sempre più importante agli inquirenti soprattutto nelle indagini complesse. E, manco a farlo apposta, a godere di questa improvvisa e inaspettata notorietà è stata soprattutto la *Digital Forensics* (traducibile solo approssimativamente con "informatica forense"): proprio la più giovane fra le discipline di indagine tecnica che, assolutamente sconosciuta ai più fino a solo pochissimi anni fa, è oggi nota a tutti almeno nei suoi principi generali di applicazione riguardanti, con grande semplificazione concettuale, gli accertamenti tecnici fatti su computer, memorie, cellulari e reti di comunicazione.

Sono tuttavia da addebitare a questa moda anche diversi aspetti negativi, che a detta di molti superano di gran lunga quelli positivi. In primo luogo si è avuto il fenomeno della

mitizzazione del ruolo del tecnico, il quale viene percepito come quantomeno cruciale se non addirittura unico responsabile della corretta soluzione del caso, in contrapposizione e soprattutto a scapito dei ruoli e dei metodi investigativi tradizionali. In secondo luogo si è invece banalizzata la disciplina stessa, diffondendo la convinzione che tutto sia ormai facile e alla portata di chiunque: basta avere un po' di software idoneo (che tanto si trova su Internet...) e qualche conoscenza informatica di base per poter fare il *forensic examiner* come e meglio dei poliziotti dei telefilm. La realtà è che le indagini tecniche sono solo un supporto al processo di accertamento della verità, utile e importante ma quasi mai esclusivo; e che i metodi e le tecniche tradizionali di investigazione, ivi compreso un sano buon senso, sono sempre preponderanti rispetto ai meri risultati degli accertamenti tecnici. Ma l'equivoco purtroppo permane, e anzi si acuisce ogni giorno di più.

A fare le spese di tali errate concezioni è soprattutto la nostra amata Digital Forensics, disciplina che viene vista da molti come più "facile" rispetto alle sue cugine anziane in quanto apparentemente non richiede conoscenze troppo specialistiche (basta "capire un po' di computer" e il gioco è fatto!). Ciò a sua volta ha dato origine a due fenomeni estremamente negativi, che stanno purtroppo generando pericolose ripercussioni pratiche nel funzionamento già precario del nostro sistema giudiziario.

In primo luogo si nota una crescente e preoccupante tendenza nei magistrati inquirenti a sopravvalutare sempre più l'importanza a fini investigativi degli accertamenti informatici, anche a scapito dell'analisi di altre prove "tradizionali"; un po' come fanno taluni medici moderni che tendono purtroppo a visitare meno i pazienti preferendo far loro effettuare una serie di accertamenti clinici strumentali. (Esempio tratto dall'esperienza personale: qualche anno fa fui chiamato da un P.M. che indagava su una reciproca denuncia per lite violenta tra due coniugi, ciascuno dei quali sosteneva di essere stato provocato dall'altro; siccome durante l'alterco lui aveva lanciato contro di lei il suo computer portatile, che oltretutto si era danneggiato nell'urto, il P.M. intendeva disporre una perizia informatica sul computer pensando così di poter ricostruire il reale andamento dei fatti e stabilire chi avesse ragione! Ovviamente rifiutai l'incarico...)

In secondo luogo, come diretta conseguenza di ciò, la crescente richiesta di perizie d'ufficio ha fatto espandere troppo rapidamente il mercato dei consulenti tecnici del giudice, che ha così inevitabilmente finito per popolarsi anche di operatori improvvisati e talvolta poco seri, che si sono buttati a pesce nel nuovo business senza tuttavia possedere le reali capacità e l'esperienza che sarebbero necessarie per poter espletare a dovere un impiego così delicato. E purtroppo la non-cultura informatica così diffusa nel nostro Paese presso chi ha una formazione umanistica fa sì che spesso i giudici e i pubblici ministeri non siano in grado di distinguere tra i consulenti davvero preparati e quelli semplicemente opportunisti, i quali tuttavia con il loro maldestro operato rischiano di orientare in modo errato e a volte tragico l'esito delle indagini. (Esperienza personale: quante volte capita che in udienza il giudice o il P.M. esordiscano dicendo al perito "cerchi di spiegarsi bene perché di computer non ci capisco niente!" o addirittura si vantino di non saperlo neppure accendere...)

La realtà è che la nostra povera Digital Forensics, la più giovane e incompresa tra le discipline forensi, è anche forse la più complessa e delicata: essa infatti unisce le difficoltà dell'investigazione a quelle tipiche dell'informatica, con tutte le complicazioni e incertezze che ben conosciamo. Il tutto, ricordiamolo bene, in un ambito di attività che in più fa ricadere sulla testa del consulente anche importanti profili di responsabilità, sia legale sia morale, relativi al proprio operato.

Perdipiù il panorama è confuso per via della giovane età della disciplina, che è tutt'ora priva di un rigoroso inquadramento tecnico-giuridico e soffre della mancanza di protocolli e linee guida unanimemente condivisi dalla comunità internazionale di esperti. Non aiuta il fatto che l'informatica stessa abbia percorso passi da gigante negli ultimi anni, trasformandosi in una sorta di bersaglio mobile impossibile da ingabbiare in regole e procedure fisse. Tanto per dire: gli accertamenti sulle impronte digitali esistono da oltre un secolo, nel corso del quale le tecniche si sono evolute e affinate ma i concetti di base non sono mutati; a paragone, invece, nei soli ultimi dieci anni l'informatica e le TLC hanno subito tante di quelle rivoluzioni, nell'hardware e nel software, da rendere obsolete diverse generazioni di sistemi. È chiaro che in queste condizioni è difficile riuscire a mantenere il diritto e la prassi allineati all'evoluzione della tecnica.

Tanti anni fa, agli albori della Digital Forensics, non c'era tanta esperienza e non c'erano tool sofisticati ma, in fondo, non servivano nemmeno: il mondo era più semplice, i sistemi più facili da analizzare e le esigenze meno complesse. Con un buon debugger e un compilatore C si poteva fare tutto ciò che serviva, a patto di essere bravi, esperti e, d'accordo, molto pazienti! Oggi invece è tutto dannatamente più complicato: le quantità di dati a disposizione di chiunque sono strabilianti, mentre i sistemi sono talmente complessi da sfuggire all'analisi dei loro stessi creatori (provate a risalire al vero motivo di un crash di Windows...).

Ecco dunque perché oggi è necessario, in questa più che nelle altre discipline forensi, disporre di una guida di riferimento che sia completa, esaustiva e soprattutto aggiornata. Nel mondo moderno chi si ferma è perduto, perché la tecnica va avanti a passi veloci. Se, tanto per fare un esempio terra terra, il massimo che poteva capitare a un perito cinque anni fa era dover acquisire e analizzare un hard disk IDE da 80 GB, oggi molto verosimilmente egli si troverà di fronte a uno storage di rete da qualche TB in RAID: una storia completamente diversa. Per non parlare di cose come cloud, virtualizzazione e via dicendo, che stanno ormai diventando la norma più che l'eccezione. Era dunque attesa una nuova edizione di questo ormai classico lavoro di Andrea "Pila" Ghirardini e Gabriele Faggioli, il primo testo sulla Digital Forensics pubblicato in Italia da italiani, divenuto ben presto un riferimento per gli addetti ai lavori. Dalla sua prima uscita a oggi sono passati sei anni, un'era geologica in termini informatici. I contenuti sono dunque stati aggiornati e ampliati ma l'impostazione è rimasta quella originale, utilmente caratterizzata da diverse chiavi di lettura: da quella strettamente tecnica a quella giuridica e legale, senza tralasciare una divertente e istruttiva carrellata di casi curiosi tratti dalla pluriennale esperienza sul campo di Andrea, che è effettivamente stato uno dei primi *forensic analyst* professionisti del nostro Paese.

Personalmente tengo molto alla divulgazione culturale dell'informatica, sia nella sua accezione generale sia nelle sue applicazioni verticali, e credo che questo libro ne sia un ottimo esempio per quanto riguarda la disciplina di cui tratta. Secondo me sbaglia chi ritiene che l'informatica sia una disciplina solo tecnica, priva di risvolti umanistici: ma sbaglia ancor di più chi ritiene tale la Digital Forensics. In essa infatti l'analista non è solo un tecnico di laboratorio o, ancor peggio, un semplice strumento nelle mani del magistrato: è invece (o dovrebbe essere) un supporto al giudice il quale, pur essendo per definizione il *peritus peritorum*, non può (e neppure deve) essere esperto in ogni branca della scienza. Il consulente o perito deve quindi supportare il magistrato nel processo di accertamento della verità sin dal momento della formulazione dei quesiti, agendo sempre in modo neutro e asettico ma non acritico, discutendo eventualmente le linee

di indagine, e stilando infine una relazione che sia non solo completa, onesta, oggettiva e veritiera, ma anche chiara e comprensibile soprattutto ai profani. Il tutto mantenendo sempre il proprio ruolo senza travalicarne i confini, perché compito del perito non è quello scrivere al giudice la sentenza ma solo quello di fornirgli con la massima chiarezza tutte le informazioni necessarie affinché egli possa giungere alle giuste conclusioni secondo il proprio libero convincimento.

Ma soprattutto l'analista dovrebbe tenere sempre presente che la sua attività, per quanto esoterica e interessante, non è un bel gioco per *geek* ma un compito delicato e gravato di responsabilità, nel quale un errore o una leggerezza possono, nei casi più gravi, significare il rilascio di un colpevole o, peggio, la condanna di un innocente. Bit e byte sono oggetti virtuali e impalpabili, ma non per questo meno "pesanti" di una traccia di DNA o di un'impronta sul luogo del delitto quando costituiscono un'evidenza a supporto di un capo d'accusa: solo, sono molto meno "leggibili" dal giudice, che quindi si affida totalmente alle conclusioni del perito. Purtroppo mi è capitato troppe volte di vedere innocenti rischiare condanne estremamente severe a causa di una perizia d'ufficio fatta male. La corretta formazione di un analista non può prescindere anche da questo ordine di considerazioni.

Corrado Giustozzi
Roma, ottobre 2013