

## Premessa

Non di rado, l'informatica viene confusa con la scienza dei *computer* e del *world wide web*, dimenticando che la materia si occupa anche di reti ed elaboratori elettronici, ma non esaurisce in tal modo il proprio ambito epistemico. Di fatti, l'informatica può essere correttamente definita come la disciplina che studia l'informazione, sia nei suoi principi generali, sia – soprattutto – nei suoi aspetti particolari, legati all'elaborazione e alla trasmissione di dati all'interno dei sistemi fisici, biologici e culturali.

Per quanto riguarda, invece, l'informatica giuridica, le origini della materia possono essere fatte risalire alla metà del secolo XX, quando *Norbert Wiener*, dopo aver coniato il termine *Cybernetics* per indicare la scienza del controllo e della comunicazione negli animali e nelle macchine, accennò ad una possibile valenza giuridica della teoria dei servomeccanismi. Qualche anno più tardi, Lee Loewinger, in un articolo pubblicato sulla *Minnesota Law Review*, affermò di voler fondare una vera e propria scienza – denominata *jurimetrics* (giurimetria) – per studiare le linee di una rete di informazione sui dati giuridici, proponendo di mettere le nuove tecnologie al servizio delle agenzie di *antitrust*.

Tuttavia, il merito di aver definito con precisione l'oggetto ed il metodo della giurimetria deve essere attribuito a Hans Baade, che, agli inizi degli anni sessanta del XX secolo, ne suddivise il campo in tre, fondamentali, ambiti di ricerca: 1) informativo (*law retrieving*); 2) previsionale (*judicial predicting*) e 3) logico decisionale (*use of symbolic logic*). Il primo di questi riguardava l'utilizzo dell'elaboratore a fini documentari, il secondo si occupava dell'analisi dei precedenti giurisprudenziali, mentre il terzo concerneva il controllo del processo decisionale seguito dal giudice. In un primo momento, l'ambito previsionale ebbe grande fortuna negli Stati Uniti – uno dei più importanti Paesi di *common law* il cui sistema giudiziale è conseguentemente incentrato sul principio dello *stare decisis* – riscuotendo minori e più timidi consensi

in Europa. Con il passare degli anni, anche gli studiosi americani finirono per abbandonare questa linea di ricerca, rassegnandosi al fatto che non è in alcun modo possibile prevedere l'esito di una controversia legale su mere basi statistiche.

Al di qua ed al di là dell'Atlantico, guadagnò invece notevole importanza l'ipotesi di modellizzazione del ragionamento giuridico così come l'ambito informativo, rappresentato dalla cosiddetta informatica giuridica documentale. Con riguardo a quest'ultimo campo di ricerca, uno dei primi e più acuti studiosi di informatica giuridica fu, senza ombra di dubbio, Spiros Simitis. Ad avviso di Simitis la professionalità di un giurista dipende, in larga parte, dalla precisione e dalla esaustività delle informazioni che egli riesce a reperire ed elaborare. Il diritto contemporaneo si caratterizza per la incontrollabile ipertrofia delle fonti normative, per il numero elevato dei provvedimenti di urgenza e per la deprecabile incoerenza logica e linguistica delle disposizioni. Per questo motivo, Simitis ritiene che gli elaboratori elettronici debbano essere messi a disposizione dei giudici, consentendo loro di adempiere correttamente alla propria funzione e di smetterla di muoversi "ancora in carrozza" all'interno di una società altamente complessa e tecnologica.

In Italia, i primi studiosi di informatica giuridica furono i magistrati che ne avviarono l'applicazione presso il CED della Suprema Corte di Cassazione. In ambito scientifico, il dibattito fu inizialmente animato dalle ricerche di Losano, Borruso e Frosini, mentre dal punto di vista strettamente accademico l'insegnamento fu da subito collocato nel settore scientifico disciplinare di pertinenza della filosofia del diritto.

Sin dalla elaborazione di questi primissimi approcci dottrinali gli studiosi di informatica giuridica sono stati impegnati nella precisa definizione delle proprie competenze e del proprio ambito di ricerca. Quel che è certo, è che la materia non può essere definita – *sic et simpliciter* – come quel ramo degli studi giuridici che si occupa delle leggi che riguardano i *computer*, ma deve più correttamente essere pensata come un Giano bifronte che si occupa tanto dell'informatica – in quanto oggetto del diritto – quanto del diritto – in quanto oggetto della rivoluzione informatica.

Di fatti, è chiaro che non esiste un ramo del diritto che non sia stato profondamente coinvolto dalla rivoluzione digitale. Per fare solo alcuni esempi, si pensi al modo in cui il processo civile telematico sta cambiando la procedura civile, alle riflessioni di diritto amministrativo e di diritto pubblico stimulate dalle procedure di consultazione elettronica

del corpo elettorale ed alle ripercussioni sui sistemi politici rappresentativi tradizionali che essi naturalmente determinano; alle provocazioni in tema di difesa della proprietà intellettuale dovute all'avvento delle reti *peer to peer*, per non parlare dei problemi connessi al valore giuridico dei documenti informatici, alla firma digitale ed alla tutela della *privacy on line*.

In definitiva, la rivoluzione digitale ha offerto interessanti spunti di ricerca praticamente in tutti i campi del diritto.

Al contempo, notiamo come l'informatica metta a disposizione dei giuristi una lunga serie di strumenti, tutti utilissimi per trattare correttamente informazioni e dati. In primo luogo, si tratta dei programmi necessari per redigere ed archiviare documenti (come, ad esempio, le leggi, le sentenze, le opinioni dottrinali o le massime giurisprudenziali); in secondo luogo, di strumenti meramente concettuali – come, ad esempio, il codice binario e l'algoritmo – che possono tornare utili per controllare la correttezza logico/formale di una legge, di una sentenza o, più in generale, di un ragionamento giuridico. Non a caso, molti studiosi auspicano che le disposizioni normative, prima di entrare in vigore, vengano sottoposte ad una specifica prova algoritmo, ciò a dire: se una norma è suscettibile di essere tradotta all'interno di un algoritmo, vuol dire che essa possiede una coerenza intrinseca, altrimenti, necessita di essere nuovamente controllata ed eventualmente revisionata, risultando evidentemente affetta da antinomie o da altre fallacie logiche.

Inoltre, l'informatica mette a disposizione dei giuristi innovativi *software* didattici – ivi inclusi i sistemi di *e-learning* –, che, integrando i tradizionali metodi di insegnamento, si ripromettono di consentire agli studenti di apprendere in maniera attiva e maggiormente coinvolgente.

Infine, informatica e diritto si “incontrano in tribunale”. Da un lato, ciò avviene grazie ai *software*, ed in particolare grazie a quei sistemi esperti che, costituendo veri e propri strumenti di arbitrato, rendono possibile la composizione alternativa delle controversie (ADR); dall'altro, questo incontro si verifica su di un piano meramente teoretico e concettuale: la diffusione dei computer, e della portentosa intelligenza artificiale di cui essi sono dotati suggerisce ai teorici del diritto di riflettere sul processo decisionale che consente al giudice di pronunciare una sentenza, discutendo sulla natura stessa del giudizio ed illuminando di una nuova luce l'antica diatriba circa la possibilità di sottoporre il ragionamento giudiziale ad un qualche tipo di controllo che ne sancisca la razionalità e la fondatezza.

Per questo motivo, è stato correttamente affermato che la giurisprudenza sta cominciando a subire da parte dell'informatica un impatto non diverso da quello subìto, e non ancora metabolizzato, dalla medicina.

Se tutto ciò è vero, è parimenti innegabile che la rivoluzione digitale determini conseguenze estremamente interessanti nel momento in cui investe uno degli aspetti più complicati della scienza giuridica: il diritto penale.

Le antiche categorie concettuali che si trovano alla base della scienza penalistica hanno sicuramente resistito all'avvento delle tecnologie informazionali. Di fatti, non vi è dubbio che le nozioni di colpa, di dolo o di tentativo – solo per fare alcuni esempi – possano essere applicate anche ai crimini informatici. Allo stesso modo, è chiaro che le antichissime questioni relative alla competenza, al luogo ed al tempo di commissione di un delitto riguardino anche – ma forse sarebbe meglio dire soprattutto – i reati informatici.

Tuttavia, non vi è chi non veda come la rivoluzione tecnologica a cui stiamo assistendo abbia influito – talvolta in maniera eclatante – su queste antiche nozioni, dotando i concetti basilari del diritto penale di una dimensione ulteriore e forse ancora non del tutto compresa ed esplorata.

Di fatti, il diritto è nato e si è sviluppato in un mondo in cui gli oggetti – materiali, tangibili e pesanti – rappresentavano la prima e fondamentale forma di ricchezza. Risulta parecchio significativa, al riguardo, la celebre novella di Verga in cui l'immenso potere di un singolo uomo viene rappresentato dalla sconfinata quantità di terre che egli possiede. Per secoli e secoli, *la roba* è stato tutto ciò di cui gli uomini avevano bisogno. Il diritto di proprietà ha dunque assunto un ruolo di fondamentale importanza nello sviluppo giuridico e culturale della società occidentale. Non solo perché esso consente di godere e di sfruttare a proprio piacere un determinato bene, ma anche e soprattutto perché la relazione di potere – esclusivo, profondo e giuridicamente tutelato – che viene ad instaurarsi tra un uomo e le cose che egli possiede serve per mediare i rapporti tra gli uomini.

In tal senso, rimane insuperata la lezione schmittiana. Come ha insegnato il celebre giurista tedesco: "l'uomo è un essere di terra che calca il suolo, questo è il suo posto e la sua posizione nel mondo". In aperta polemica con le potenze di mare, preconizzando che la globalizzazione avrebbe presto conquistato il mondo sotto la specifica cifra della tecnologia, Carl Schmitt ha ribadito che la giustizia è, per essenza, terranea. Solcare un confine sulla terra rappresenta il primo e fondamentale atto

attraverso il quale gli uomini provano ad ordinare l'ambiente in cui vivono. Dal momento in cui il confine, segnando la distinzione tra amico e nemico, trasforma la terra in un vero e proprio territorio, il tempo e lo spazio guadagnano senso ed uno specifico orientamento.

Per questo motivo, la proprietà privata richiede di essere tutelata giuridicamente, assurgendo a bene giuridico di primissimo piano, degno, in caso di aggressione, di scomodare la *extrema ratio* del diritto penale.

Eppure, la rivoluzione digitale ha modificato in maniera radicale la situazione sin qui descritta. In primo luogo, perché l'avvento delle reti ha fatto crollare le frontiere nazionali, consentendo ai pirati informatici di commettere crimini in terra straniera e di sfuggire alle frontiere con relativa facilità. In secondo luogo, l'avvento dell'era informazionale ha modificato radicalmente i desiderata dei cittadini. Non vi è dubbio che la ricchezza, oggi, non si misuri sulla base della quantità di oggetti – tangibili, reali, pesanti – che un uomo possiede; né, tantomeno, sulla estensione delle sue terre. Il bene più prezioso è oggi l'informazione. Il denaro, la letteratura, l'arte ed il cinema, queste come mille altre cose sono state sottoposte ad un processo di smaterializzazione che ha reso molto più facile produrre, accumulare e trasmettere ricchezza alla velocità della luce. Sotto forma di *bit*.

In tal senso, la rivoluzione digitale sembrerebbe aver comprovato l'antica profezia marxiana in base alla quale ogni cosa sarebbe divenuta un giorno volatile.

Posto di fronte ad una simile *liquefazione*, lo studioso del diritto – ed in particolar modo del diritto penale – non può non avvertire un senso di spaesamento e di vertigine. Anche la ricchezza digitale richiede di essere tutelata: il traffico planetario di dati, informazioni e programmi che transitano senza sosta sul *world wide web* necessita di essere organizzato e disciplinato. Tuttavia, è molto più difficile intercettare un *file* che una partita di droga; è molto più difficile sequestrare un milione di bit che mettere sotto sequestro una barca, è molto più difficile far acquisire agli atti un archivio informatico – senza inquinare maldestramente il valore probatorio –, piuttosto che una pistola o un pugnale.

Anche se volessimo provare a mettere tra parentesi il necessario ripensamento delle categorie penalistiche relative al fatto, al luogo ed al tempo di commissione di un delitto, dovremmo riconoscere che l'avvento dell'era informazionale ha cambiato alcuni fondamentali concetti di uso comune, costringendo il legislatore penale a rivedere le nozioni concettuali su cui sono state costruite molte e diverse fattispecie.

Pensiamo, ad esempio, al concetto di domicilio. Un tempo, questo ambito territoriale di esclusiva pertinenza di un cittadino possedeva confini certi e facilmente identificabili – al massimo, sarebbe stato possibile discutere sulla nozione di pertinenza o sulla legittimità degli *offendicula*. Oggi, la nozione di domicilio è stata giustamente arricchita di una ben più problematica dimensione digitale. Il legislatore ha stabilito che ogni cittadino ha diritto alla tutela del proprio domicilio informatico, i confini di quest'ultimo, tuttavia, sono ogni giorno più difficili da identificare e difendere – basti pensare al recente avvento del *cloud computing* ed allo sconfinato campo di ricerca che esso apre.

Ancora, poniamo mente al concetto di pornografia virtuale. Il legislatore ha ritenuto di dover sanzionare penalmente anche la detenzione, il commercio, la diffusione e la produzione di immagini che sembrano vere, ma che, essendo state ritoccate con uno specifico programma informatico, non rappresentano situazioni realmente verificatesi. Da ultimo, riflettiamo sul reato di truffa. Prima della rivoluzione informatica, questa fattispecie penalistica risultava saldamente ancorata al contegno intersoggettivo del soggetto agente – teso a far cadere qualcuno in errore grazie alla commissione di artifici o raggiri. Con l'avvento dell'era digitale si sono andate moltiplicando le truffe ai danni degli elaboratori elettronici – dalla clonazione di utenze telefoniche mobili alla manomissione dei bancomat. In un primo momento, tutto ciò ha costretto la giurisprudenza ad interpretare fantasiosamente il requisito della forzosa collaborazione della vittima. Successivamente, ha imposto la creazione di un nuovo articolo del codice penale, in grado di sanzionare il comportamento fraudolento del reo a prescindere da un reale contatto interazionale con la vittima.

La rivoluzione digitale ha posto dunque il legislatore penale di fronte ad almeno due emergenze, parimenti problematiche e significative. La prima è stata quella di capire come proteggere i computer, le reti, i dati e le informazioni in esso contenuti; la seconda è stata quella di approntare una normativa in grado di tutelare i cittadini da quelle condotte criminali che, pur non avendo ad oggetto un computer, possono essere portate a compimento grazie ad uno scorretto utilizzo dei computer e delle reti.

In tal senso, la dottrina usa distinguere i reati propriamente informatici dai reati *lato sensu* informatici. Con la prima categoria concettuale si fa solitamente riferimento a quei reati che esistono perché esistono i computer – se non esistessero gli elaboratori elettronici, non sarebbe di fatti concepibile la diffusione di virus informatici o il possesso abusivo

di codici d'accesso. Con la seconda categoria si usa invece fare riferimento a quei reati che hanno guadagnato una specifica e perniciosa diffusione a causa della rivoluzione digitale, pur aggredendo ben più antichi beni giuridici – come, ad esempio, il patrimonio, la personalità o la riservatezza.

Pur essendo molto utilizzata, la *summa divisio* a cui si è appena fatto cenno vale in linea di massima: può tornare utile per fornire allo studioso un primissimo criterio orientativo, ma non è in grado di essere applicata a tutte le fattispecie e di qualificare con precisione tutte le condotte criminose. Risulta paradigmatico, in tal senso, il caso della frode informatica: se da un lato la condotta criminale aggredisce innegabilmente il patrimonio della vittima, dall'altro, le modalità commissive indicate nella fattispecie legale non possono in alcun modo prescindere dalla esistenza di un elaboratore elettronico.

Allo stesso modo, merita di essere adottata *secundum quid* la distinzione tra reati nei quali il computer è un mezzo e reati nei quali il computer è oggetto della condotta. Se non altro perché in molti reati informatici l'elaboratore elettronico rappresenta sia il mezzo che l'oggetto dell'azione criminale.

Quel che è certo è che l'avvento di internet ha dato luogo ad una enorme quantità di interazioni, consentendo agli utenti della rete di sfruttare molte opportunità ed esponendoli contemporaneamente a molte minacce: dal *phishing* allo *sniffing*; dal *pharming* al *defacing*, al *cyber-squatting*. Per non parlare della allarmante diffusione di *virus* e *malware*, come, ad esempio, gli *adware*, le *logic bomb*, le *time bomb*, i *worm* o i *trojan horse*. Fortunatamente, sono andati crescendo anche i sistemi di sicurezza e gli strumenti di controllo, alimentando una guerra senza esclusione di colpi tra i pirati informatici e le forze di polizia.

Per inciso, notiamo che molti strumenti di sicurezza informatica possiedono un aspetto, per dir così, oscuro e negativo – dato che possono essere utilizzati per combattere il crimine, ma possono anche essere sfruttati dai governi e dalle multinazionali per controllare illecitamente l'attività dei cittadini, spiandone le interazioni virtuali per finalità commerciali o politiche.

Infine, l'informatica promette innovazioni e stravolgimenti anche per quanto riguarda i sistemi sanzionatori. Nel corso degli ultimi secoli, siamo passati dalla cruenta spettacolarità dei supplizi alla intangibilità del corpo del condannato, considerando quest'ultimo principio alla stre-

gua di un segno di inequivocabile civiltà e progress. Oggi, la tecnologia informatica consente una rivoluzione ulteriore ed altrettanto importante, mettendo a disposizione delle forze dell'ordine tutta una serie di strumenti che permettono di controllare l'attività del reo anche fuori dagli angusti confini di una cella, rendendone il corpo sempre visibile e tracciabile – se il braccialetto elettronico è già molto diffuso ed utilizzato, non sembra mancare molto all'impianto di veri e propri chip sottocutanei.

\* \* \*

La prima parte di questo lavoro è dedicata agli aspetti di teoria generale connessi alla criminalità informatica. Al suo interno, il lettore troverà un resoconto delle principali minacce informatiche ed un riferimento alla giurisprudenza in tema di reati informatici. La seconda parte, invece, è dedicata all'analisi delle principali figure criminose presenti nel codice penale. Al suo interno, il lettore troverà alcuni spinosi problemi interpretativi ed altrettante questioni dottrinali connesse alle condotte di accesso abusivo a sistema informatico, diffusione di virus, frode informatica e detenzione di immagini pedopornografiche.

L'intento degli autori è stato di contribuire ad illuminare un ramo del tutto peculiare dell'informatica giuridica, approntando un manuale ad uso di lezioni dedicato, in prima istanza, ad essere studiato dai giuristi di domani: gli alunni del corso di laurea magistrale in Giurisprudenza.

*Agata C. Amato Mangiameli  
Guido Saraceni*

Roma, 20 dicembre 2018