

TCRS

Teoria e Critica della Regolazione Sociale

Quaderno 2012

Federico Puppo

PROVA DIGITALE E LOGICA GIURIDICA:
L'INFORMATICA DEL DIRITTO
DA UNA PROSPETTIVA RETORICA

Centro Studi TCRS

Via Crociferi, 81 - 95024 Catania - Tel. +39 095 230478 - tcrs@lex.unict.it

Federico Puppo
Università di Trento
federico.puppo@unitn.it

In:
Libertà e buon governo
Quaderno 2012

ISSN: 1970-5476
Centro Studi
"Teoria e Critica della Regolazione sociale"
Via Crociferi, 81 - 95024 Catania
Tel. +39 095 230478 – Fax +39 095 230462
tcrs@lex.unict.it
www.lex.unict.it/tcrs

Federico Puppo

PROVA DIGITALE E LOGICA GIURIDICA: L'INFORMATICA DEL DIRITTO
DA UNA PROSPETTIVA RETORICA¹

§1. Introduzione.

In questo lavoro ci proponiamo di sviluppare un'indagine nel campo dell'informatica del diritto (o informatica giuridica), ovvero di quel settore della filosofia del diritto che, approssimativamente, si preoccupa di riflettere intorno all'impatto dispiegato dall'impiego di strumenti informatici nel diritto².

A tal fine è tuttavia opportuno enunciare alcuni presupposti del nostro discorso, che per ragioni di spazio non potremmo argomentare come vorremmo ma che certamente è doveroso palesare, delimitando nel contempo il campo della nostra riflessione.

In primo luogo ricordiamo così come, per noi, trattare di diritto voglia innanzitutto dire trattare di processo, ossia prendere in considerazione quella forma peculiare di esperienza che si presenta come un dialogo organizzato in guisa di controversia di fronte ad un terzo chiamato a risolverla³. Il diritto, in effetti, nella tradizione Occidentale si è sin da subito, sin dalle *Eumenidi* di Eschilo, manifestato come processo, ovvero come scontro di pretese opposte di fronte ad un giudice terzo ed imparziale, chiamato a dirimere la lite: cioè a dire chi, fra i contendenti, abbia ragione⁴, nel rispetto di una logica idonea a governare e controllare i discorsi di parte, dovendo tenere conto delle acquisizioni probatorie e delle qualificazioni giuridiche che il contraddittorio processuale sia stato capace di mettere in campo e

¹ I contenuti del presente lavoro sono stati anticipati in lingua portoghese in un articolo in pubblicazione sulla «Revista Brasileira de Estudos Constitucionais – RBEC», Belo Horizonte, Minas Gerais, Brasil, 7.26, maio/agosto 2013.

² Per l'esposizione delle differenze che sussistono fra l'informatica del diritto ed il diritto dell'informatica v. ad es. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, Torino: Giappichelli, 2012, in part. pp. 16-41; M. COSSUTA, *Questioni sull'informatica giuridica*, Torino: Giappichelli, 2003, in part. pp. 13-66; M.G. LOSANO, *Sistema e struttura nel diritto. Volume III. Dal Novecento alla postmodernità*, Milano: Giuffrè, 2002, in part. pp. 1-115.

³ Per un approfondimento del tema v., fra altri, M. MANZIN, *In principio era il contraddittorio. «La giustizia penale»*, 51, 2010, pp. 397-406; F. PUPPO, *Informatica giuridica e metodo retorico. Per un approccio "classico" all'uso delle nuove tecnologie*, Trento: Tangram, 2012, in part. cap. 2.

⁴ E. RIPEPE, *Civiltà giuridica europea e retorica giudiziaria: un'anteprima a teatro*, in M. MANZIN, F. PUPPO (a cura di), *Audiatur et altera pars. Il contraddittorio fra principio e regola*, Milano: Giuffrè, 2008, pp. 63-95; F. CAVALLA, *All'origine del diritto Al tramonto della legge*, Napoli: Jovene, 2011 (in part. pp. 93-159).

selezionare⁵. Dove, nella concezione che facciamo nostra, il contraddittorio appare, «più che una *regola* processuale, vero e proprio *principio* dell'ordinamento»⁶, identificando l'*eidòs* di ogni processo e senza il quale, quindi, questo non potrebbe neppure esistere.

Un tanto chiarito, precisiamo in secondo luogo che, volendo interrogarci intorno ai problemi connessi all'utilizzo di strumenti informatici all'interno del diritto (*rectius*: del processo), volgeremo la nostra attenzione al tema della prova digitale per cercare di comprendere se, ed in che misura, le problematiche poste dalle nuove tecnologie informatiche siano capaci, a volte anche in modo non manifesto, di influire sul e condizionare il processo: intendendo con questo riferirci non tanto e non solo alla sua dimensione normativo-procedurale (di cui anzi non ci occuperemo affatto)⁷, ma proprio alle sue struttura essenziale e logica intrinseca, che rischiano di uscirne viziate e compromesse.

§2. Logica informatica e logica giuridica.

Senza che ci si possa qui soffermare troppo sul punto, basti a questo proposito ricordare come tra la logica propria dell'informatica e quella propria del diritto è possibile registrare alcune importanti differenze.

In effetti, la logica booleana cui è improntato lo sviluppo e l'impiego degli strumenti informatici è un tipo di logica che si caratterizza per ipoteticità, deduttività e monologicità⁸. I ragionamenti che interessano tale logica si sviluppano, cioè, da premesse convenzionalmente stabilite e presupposte *a priori*, che costituiscono la complessa rete di istruzioni fornite ai sistemi informatici sotto forma di algoritmo, nell'esecuzione di alberi di inferenze deduttive in cui il nesso tra premesse e conclusioni gode di ripetibile ed inalterabile monoticità grazie alla normalizzazione e formalizzazione del linguaggio naturale e delle regole logiche che governano i nessi inferenziali.

⁵ Cfr. M. MANZIN, *Quale logica per il processo penale? Ragionamento giudiziale e forme di controllo argomentativi della sentenza*, in V. COMI, G. DOMINICI (a cura di), *L'argomentazione giudiziale e il suo controllo in Cassazione. Atti del Convegno, Lipari 10 settembre 2011*, Roma: Aracne, 2012, pp. 63-79.

⁶ M. MANZIN, *Del contraddittorio come principio e come metodo/On the adversarial system as a principle and as a method*, in M. MANZIN, F. PUPPO (a cura di), *Audiat et altera pars*, cit., pp. 3-21: 13.

⁷ Rimandiamo per tal fine alla recente ed attenta analisi di G. DI PAOLO, *vc. La prova informatica (diritto processuale penale)*, Enciclopedia del diritto. Annali VI, Milano: Giuffrè, 2013, pp. 736-762.

⁸ Per un primo esame rimandiamo, fra altri, a P. MORO, *L'informatica forense. Verità e metodo*, Torino: San Paolo, 2006, in part. pp. 40ss, da cui anche l'enunciazione delle caratteristiche testé richiamate e la breve analisi che ne proponiamo.

Si tratta di una logica assai potente e controllabile ma che, per molti versi, poco si attaglia alla natura argomentativa del diritto, e del processo in particolare, che implica invece una logica retorica di tipo anipotetico, argomentativo e dialogico⁹. Ossia una logica che conosce ragionamenti che partono da premesse di tipo endossale e che giungono alle conclusioni non *per modum deductionis*, ma per via argomentativa e dialettica, dovendo tenere conto degli attacchi e delle tesi avversarie, che vanno confutate.

Si tratta, è evidente, di due modelli di logica diversi e concorrenti¹⁰, ma secondo noi non necessariamente escludentisi. A nostro modo di vedere, infatti, tali logiche possano, per così dire, “collaborare” nel contesto del processo: ma solo a patto che il ruolo principale lo giochi la logica retorica di tipo classico, in cui, come proveremo a mostrare nel prosieguo, quella informatica di tipo moderno può in certo modo essere inclusa. Ciò che invece non è possibile fare è ridurre al rango di discorsi analitico-deduttivi i discorsi di tipo argomentativo, pena la perdita di identità del diritto e del processo: l’impiego di ogni tecnologia, e di quella digitale in particolare, non è, infatti, un’operazione neutra, ma è capace di mutare profondamente la natura stessa di ciò a cui è applicata. E questo emerge con piena evidenza proprio guardando al modo in cui l’impiego di sistemi informatici è stato capace di modificare radicalmente non tanto il processo, ma addirittura il sapere deduttivo per eccellenza, e cioè quello matematico.

§3. L’incidenza della tecnologia digitale nel sapere matematico...

Nella nostra prospettiva, caratterizzata dagli elementi sinora richiamati, trattare della prova digitale vuol dire guardare all’esperienza concreta della prassi forense: e se fosse vero che la tecnologia non è neutrale, dovremmo aspettarci di incontrare un qualche cambiamento di paradigma teorico, capace di modificare (in

⁹ Si v. ancora *ibidem*, p. 67ss.

¹⁰ Ne abbiamo più diffusamente trattato nel nostro F. PUPPO, *Dalla vaghezza del linguaggio alla retorica forense. Saggio di logica giuridica*, Padova: Cedam, 2012, in part. cap. 6, dove abbiamo messo in luce come la logica booleana moderna è governata dal principio di identità mentre quella retorico-aristotelica classica dal principio di non contraddizione. Per un approfondimento sulla natura dei due modelli di sapere e sulle ragioni teoretiche che hanno portato al formarsi di quello moderno v., su tutti, M. MANZIN, *Ordo Iuris. La nascita del pensiero sistematico*, Milano: Franco Angeli, 2008.

atto o almeno in potenza) la natura del contraddittorio, ovvero di quel modo di acquisizione della prova che corrisponde alla natura retorica del diritto¹¹.

Per comprendere la questione il modo migliore è, come anticipavamo in chiusa la paragrafo precedente, prendere le mosse da un problema totalmente extra-giuridico che però pone la questione dell'utilizzo di sistemi di calcolo informatico in un sapere, quello della matematica, che dovrebbe sembrare totalmente impermeabile alla cosa, se non altro perché esso stesso è calcolo. Ci si può quindi legittimamente attendere che se l'impiego di sistemi informatici non è stato indolore per la matematica – la quale ha la stessa natura analitico-deduttiva dei sistemi informatici che dalla logica matematica sono nati –, lo sia ancor di meno per il diritto – che, come abbiamo detto, ha natura completamente diversa.

Ma andiamo con ordine e vediamo, in primo luogo, quale tipo di problemi si sono presentati nel contesto delle teorie matematiche per poi comprendere che tipo di riflessi tutto ciò possa avere per il diritto¹².

Come noto, uno dei teoremi matematici che, a dispetto della sua apparente banalità, è rimasto irrisolto per più di un secolo è il c.d. "teorema dei quattro colori", che è stato definito «il più famoso ed affascinante teorema della teoria dei grafi»¹³. Il teorema afferma che, data una carta geografica o una qualunque superficie piana divisa in regioni adiacenti (che abbiano cioè, per definizione, almeno in comune un segmento e non solo un punto o più punti isolati), per colorare gli stati o regioni adiacenti in modo tale che essi non presentino lo stesso colore sono sufficienti e necessari solo quattro colori. Se è stato piuttosto semplice verificare che tre colori non sono sufficienti, lo è stato assai meno provare che ne servono certamente cinque: ma il vero problema fu dimostrare che ne bastano solo quattro.

La congettura pare fosse nel 1840 già nota a Möbius, ma la sua "data di nascita" sembra essere il 1852, quando uno studente di De Morgan, Francis Guthrie, ne mise a parte il proprio insegnante che però, incapace di dimostrarla, la

¹¹ Come espressamente previsto, ad es., dall'art. 111 della Costituzione Italiana che recita: «1. La giurisdizione si attua mediante il giusto processo regolato dalla legge./2. Ogni processo si svolge nel contraddittorio tra le parti, in condizione di parità, davanti a un giudice terzo e imparziale. [omissis] 4. Il processo penale è regolato dal principio del contraddittorio nella formazione della prova. [omissis]».

¹² Ampliamo ed approfondiamo in questa sede quanto già in parte trattato in P. MORO, F. PUPPO, *Informatica e retorica forense*, «Tigor - Rivista di scienza della comunicazione», 2, 2010, pp. 67-75 (disponibile on line: <www.rivistatigor.scfor.units.it>. Accesso il 12 ottobre 2012): 72ss.

¹³ A. PASOTTI, *Il teorema dei quattro colori e la teoria dei grafi*, «Matematicamente», 1.4, pp. 7-10 (disponibile on line: <www.matematicamente.it/magazine/ottobre2007/Numero04.pdf>. Accesso il 12 ottobre 2012): 7.

propose alla *London Mathematical Society*, senza però trovare qualcuno in grado di risolverla: la storia della ricerca della soluzione conobbe così diverse e numerose tappe, con molti fallimenti e piccole conquiste, e quindi diversi risultati parziali. Qui ovviamente non interessa ripercorrere nel dettaglio l'evoluzione della cosa: è invece essenziale mettere in evidenza come solo nella seconda metà del Novecento fu possibile raggiungere la dimostrazione della congettura originaria, che assurse pertanto al rango di teorema. Ed il modo in cui ciò fu finalmente possibile, che forse spiega anche perché, in precedenza, nessuno fu mai capace di ottenere quel risultato, ha dell'incredibile.

La dimostrazione fu infatti ottenuta solo nel 1976, quando Kenneth Appel e Wolfgang Haken, due ricercatori dell'Università dell'Illinois, annunciarono di avere finalmente provato la congettura dopo quattro anni di lavoro congiunto. Essi furono così in grado di dimostrare che, effettivamente, il numero minimo di colori necessari per colorare una mappa senza che due regioni limitrofe abbiano il medesimo colore è quattro. La cosa che però più colpì la comunità dei matematici fu infatti il *modo* in cui Appel e Haken pervennero alla dimostrazione, giacché essa fu possibile solo grazie l'utilizzo di un *computer*. Infatti,

«la loro dimostrazione si basa sulla riduzione del numero infinito di mappe possibili ad un numero finito, per l'esattezza 1.476, di configurazioni per le quali la validità del teorema viene verificata caso per caso grazie ad un complesso algoritmo informatico [...]. Nel 1976 il teorema era dimostrato. Il programma definitivo aveva avuto ben 500 variazioni da quello originario e fu eseguito su due macchine diverse con algoritmi indipendenti al fine di ridurre al minimo la possibilità di errore. Per analizzare tutti i casi possibili i computer impiegarono circa 1200 ore e servirono più di 500 pagine per trascrivere a mano tutte le verifiche che costituivano la dimostrazione»¹⁴.

Da questo punto di vista il 1976 è una data fondamentale nella storia della matematica perché, per una delle prime volte, la validità di un teorema fu provata da catene di calcolo eseguite da un computer che, per definizione, esclude la possibilità di controllo diretto da parte dell'uomo. D'altra parte non v'era altra

¹⁴ *Ibidem*, p. 10.

soluzione possibile, poiché «la quantità di calcoli richiesta era tale da rendere impossibile il controllo di ogni passaggio da parte di un matematico umano»¹⁵.

Ma il cambiamento di paradigma fu enorme: in effetti, anche (ma verrebbe da dire persino) nella matematica, l'utilizzo di sistemi informatici non può essere considerato neutrale e cambia la natura stessa della dimostrazione. Infatti,

«fino ad allora, una dimostrazione consisteva in un ragionamento logicamente corretto mediante il quale un matematico poteva convincere un altro della verità di qualche asserzione. Leggendo una dimostrazione, un matematico poteva persuadersi della verità dell'affermazione in questione ed anche arrivare a capire la ragioni che ne sostenevano la validità. [...] Invece, nella dimostrazione della congettura dei quattro colori l'uso del calcolatore era assolutamente indispensabile: la prova era imperniata proprio su questo. Per accettare la dimostrazione occorre essere convinti che il programma impiegato esegua ciò che i suoi autori affermano»¹⁶.

In effetti, come dicevamo, il controllo della dimostrazione svolta dal calcolatore fu possibile solo «mediante l'esecuzione su di un'altra macchina di un programma scritto in maniera indipendente. [Ma] una parte critica della dimostrazione rimaneva così nascosta agli occhi umani»¹⁷: il risultato fu che, per molti matematici, la dimostrazione fornita da Appel e Haken non poteva a rigore essere considerata una dimostrazione, dal momento che i risultati ottenuti non potevano in alcun modo essere verificati dall'uomo.

E in effetti, poiché la complessità dei calcoli impiegati è molto alta, «persino i sostenitori delle dimostrazioni assistite dal calcolatore devono ammettere che gli oppositori dispongono di qualche ragione a sostegno delle loro opinioni»¹⁸. Non si deve peraltro ignorare il fatto che è possibile contestare la validità di una

¹⁵ K. DEVLIN, *Mathematics: The New golden Age*, London: 1988 (= *Dove va la matematica*, nuova edizione riveduta e ampliata, tr. it. di A. Giannetti, A. Manassero, riveduta da L. Servidei. Torino: Bollati Boringhieri, 1999, I ristampa 2005), p. 174.

¹⁶ *Ibidem*, pp. 174s. Si noti così come, anche nella matematica, possano presentarsi affermazioni di tipo argomentativo-retorico, come quelle che abbiamo evidenziato nella citazione appena riportata, con ciò rendendo possibile riconsiderare gli stessi termini del rapporto fra scienza e retorica, superando l'immagine della divisione fra le due. Ci sia per questo permesso rimandare alle considerazioni che sul punto svolgiamo nel nostro F. PUPPO, *Vaghezza del linguaggio e retorica forense*, cit., e alla bibliografia ivi citata.

¹⁷ K. DEVLIN, *Mathematics*, cit., p. 175.

¹⁸ *Ibidem*, p. 176.

dimostrazione eseguita con il computer «non solo per l'impossibilità di verifica manuale, ma anche perché la logica afferma che è impossibile dimostrare la correttezza di un algoritmo»¹⁹: la Tesi di Church-Turing, che è per così dire il "corrispettivo" dei Teoremi di Gödel per la teoria della computabilità, stabilisce infatti che «esistono problemi i quali, *neppure in linea di principio*, non possono essere risolti con un algoritmo. Ad esempio, non può esistere alcun programma che sia in grado di stabilire in generale se un programma qualsiasi con un certo input terminerà il suo calcolo o meno»²⁰. In effetti,

a) «non esiste alcun metodo preciso (algoritmico) che garantisce l'individuazione di ogni errore in qualsiasi programma»²¹: è questa la conseguenza più immediata dell'impossibilità di risolvere il c.d. "problema della fermata" così come dimostrata da Alan Turing;

b) «normalmente non è possibile verificare la correttezza di un algoritmo applicandolo preventivamente a ogni input possibile»²²: infatti, proprio come non è possibile stabilire preventivamente quali e quanti casi possono cadere sotto l'applicazione di una norma o di un insieme di norme, così non è possibile preventivamente stabilire quali e quanti siano tutti gli input possibili, che potrebbero essere o infiniti o anche così numerosi da risultare incalcolabili;

c) «un algoritmo può operare correttamente nella maggior parte dei casi, ma cadere in errore rispetto a input particolari»²³: ma noi sapremo quali sono questi input che producono errore solo quando li incontriamo: infatti, finché non si incontrano tali input non si può sapere quali essi siano, perché come abbiamo appena detto non è possibile stabilire anticipatamente quanti e quali siano gli input possibili.

Tutti questi aspetti sono naturalmente molto delicati perché pongono, tra l'altro, il problema della responsabilità, ossia di chi debba rispondere laddove si verifichi un errore nel caso di utilizzo di strumenti informatici: se chi ha progettato l'algoritmo (ma sembrerebbe difficile poterlo affermare, perché si tratta di limiti intrinseci tali da liberare da colpa chi progetta algoritmi) o la macchina che lo

¹⁹ A. PASOTTI, *Il teorema dei quattro colori*, cit., p. 10.

²⁰ M. FRIXIONE, D. PALLADINO, *Funzioni, macchine, algoritmi. Introduzione alla teoria della computabilità*, Roma: Carocci, 2004, pp. 225; 248; 375.

²¹ G. SARTOR, *L'informatica giuridica*, cit., p. 102.

²² Loc. ult. cit.

²³ Loc. ult. cit.. Tralasciamo per brevità il problema dell'efficienza degli algoritmi, cioè di quanto tempo possa impiegare un processo di esecuzione per giungere al termine.

processa (ma si potrebbe fare la stessa osservazione) o il soggetto che usa la macchina (e qui forse potrebbero sorgere maggiori perplessità) o tutti e tre. Si tratta di quella serie di problemi che rientrano nel campo della c.d. "tecnoetica", che certamente qui non intendiamo trattare, ma che a nostro giudizio occorre avere presenti²⁴. Anche perché, prima o poi, il diritto sarà chiamato a dover disciplinare anche tale settore, valutando se le norme giuridiche finora in essere risultino insufficienti o meno: ma certamente lo saranno se si ignoreranno i limiti logici di qualsiasi sistema artificiale, che a volte finiscono con l'essere mascherati dalle potenzialità tecniche degli strumenti digitali cui sottostanno.

Tutto ciò è emerso molto chiaramente proprio nel caso della dimostrazione del teorema dei quattro colori, insieme a considerazioni di tipo sorprendentemente *estetico*. Ricordiamo, infatti, che «fino ad oggi nell' algoritmo [che ha fornito la base di calcolo per la dimostrazione del teorema] non è stato trovato alcun errore; ad ogni modo anche se ne viene accettata la validità, la dimostrazione non è certo elegante. Come disse un critico "una buona dimostrazione matematica è come un poema, questa è un elenco telefonico!"»²⁵.

Ebbene, a noi pare che se l'utilizzo di sistemi informatici all'interno delle dimostrazioni matematiche può rappresentare un problema – perché incide sulla stessa *natura* delle dimostrazioni – lo stesso possa dirsi qualora sistemi informatici vengano utilizzati nel contesto giuridico processuale – ove potrebbero mutare la natura del confronto dialettico fra le parti e così trasformarne radicalmente la struttura. Lo abbiamo appena visto: se nel caso della dimostrazione del teorema dei quattro colori uno dei rilievi avanzati dalla comunità dei matematici era che quella non potesse essere considerata una vera e propria dimostrazione (perché nessun uomo può verificarne i passaggi e sottoporli a critica, per essere poi eventualmente convinto della correttezza delle argomentazioni svolte), ancora più l'occorrenza di tale situazione diventa grave nel contesto dialogico-controversiale del processo: e questo, come subito vedremo, è esattamente quello che succede nel campo della prova digitale.

²⁴ Per un primo esame di tali questioni si v., *ex multis*, A. MONTANARI, *Questioni di tecnoetica in intelligenza artificiale, robotica e bionica*, in P. MORO, *Etica Informatica Diritto*, cit., pp. 33-50.

²⁵ A. PASOTTI, *Il teorema dei quattro colori*, cit., p. 10. Si osservi nuovamente che se nella matematica ha un qualche rilievo l'aspetto estetico delle dimostrazioni, allora probabilmente le connessioni con il sapere retorico sono più profonde di quanto non abbia fatto vedere l'impostazione semplicistica della modernità che separa nettamente i due saperi.

§4. ...e in quello giuridico-processuale: la prova digitale...

Fa parte, ormai, della conoscenza comune, alimentata anche da racconti, fatti di cronaca, film e programmi televisivi, il fatto che la diffusione dei computer, della rete Internet e della posta elettronica – per non parlare di quelli che sono stati chiamati «media non convenzionali e gadget elettronici»²⁶ – ha portato il mondo digitale direttamente sulla *scena criminis*. Il diritto penale ha così dovuto confrontarsi con nuove figure di reato e, allo stesso tempo, la procedura penale ha dovuto fornire le regole per regimentare istituti che, toccati dalle nuove tecnologie, hanno mutato la propria natura, come è stato appunto il caso delle c.d. “prove digitali”²⁷. Espressione con cui si indicano genericamente quegli elementi idonei ad accertare il reato che siano non solo da ricercare nei più vari supporti di memorizzazione dei dati informatici, ma siano da essi stessi costituiti.

In via più generale, in questo contesto si parla comunemente di *computer forensic science*, o più brevemente di *computer forensics*, intesa come «*the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media*»²⁸. Una definizione, come si vede, assai ampia e generica, al pari di quella di “traccia elettronica o informatica” ché, «in generale, quando si parla di “*digital evidence*” si vuole richiamare l’attenzione sulle informazioni ed i dati conservati o trasmessi dalle apparecchiature cosiddette digitali»²⁹, senza potere tuttavia concepire un elenco chiuso di esempi.

Il settore è in effetti nuovo ma è anche condizionato da tecnologie in continua evoluzione e dal fatto che mancano normative chiare, capaci di dettare norme precise per questa fase istruttoria (che anche se ci fosse finirebbe presto con il diventare obsoleta), non esistendo neppure indirizzi giurisprudenziali concordati o una standardizzazione delle procedure a livello operativo, e quindi quella *best*

²⁶ A. GHILARDINI, G. FAGGIOLI, *Computer Forensic*, Milano: Apogeo, 2007, pp. 309ss, ove si discute di dispositivi come i lettori *mp3* (es. iPod), *consolle* portatili (es. Sony PSP), *smartphone* (es. iPhone) ecc.

²⁷ Per un esame delle quali rimandiamo ancora una volta a G. DI PAOLO, *vc. La prova digitale*, cit., e alla bibliografia ivi citata.

²⁸ M.G. NOBLETT, M.M. POLLITT, L.A. PRESLEY, *Recovering and Examining Computer Forensic Evidence*, «Forensic Science Communications», 2.4, 2000 (disponibile on line: <<http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm>>. Accesso il 30 ottobre 2012), p. 2.

²⁹ G. COSTABILE, *Scena criminis, documento informatico e formazione della prova penale* (disponibile on line.: <<http://www.penale.it/page.asp?mode=1&IDPag=72>>. Accesso il 30 ottobre 2012), p. 2.

practice della scienza cui occorre far riferimento in presenza di nuove prove scientifiche, come sono quelle di cui qui stiamo trattando³⁰.

Fra i problemi che sono stati affrontati e discussi, v'è quello relativo alla necessità di dover garantire e dimostrare l'integrità dei dati raccolti sui supporti digitali, che ovviamente non possono venire modificati *ante* processo, pena la nullità o comunque la contestabilità della validità prova stessa. Il punto è però che la stessa acquisizione di una prova digitale, per la sua natura, rischia di produrre quel risultato indesiderato poiché si potrebbe intaccare il supporto su cui è contenuta, modificandolo: ed ecco perché si pretende che l'esame della prova venga effettuato non sull'originale del supporto ma sulla sua «copia forense [che] ha lo scopo di effettuare una duplicazione 1 : 1 del supporto incriminato»³¹. Si parla, in questi casi, di *legal imaging* del supporto che contiene non solo i dati ma tutte le informazioni in esso contenute e che «dovrà essere necessariamente validata, ovvero confrontata con l'originale per sincerarsi della sua perfetta corrispondenza»³². Si tratta, come noto, di una copia ottenuta con un processo informatico ad "alta soglia di garanzia" il quale consente «di operare su un *hard disk* praticamente identico all'originale, sia in maniera logica che fisica, quindi anche su eventuali parti presumibilmente vuote dello stesso, che potrebbero contenere file o frammenti di file cancellati non sempre visibili con i normali strumenti di *windows*»³³.

Per evitare di alterare la traccia informatica è pertanto necessario adoperare particolari procedure ed utilizzare idonei strumenti *software*, così da evitare dubbi circa l'integrità dei dati in questione: ad esempio, deve essere utilizzato un *hard disk* nuovo oppure sottoposto ad una previa operazione di *wiper*, dovendo peraltro il sistema operare in modo non invasivo con l'ausilio di un blocco di scrittura. Potendo ignorare altre problematiche, ciò che ci sembra particolarmente rilevante è che la *legal imaging* va per così dire "sigillata" in modo tale che si abbia la certezza che quella sia effettivamente la copia completa e perfetta del supporto digitale. Come noto, questo avviene tramite l'apposizione di un «"marchio digitale" [...] creato con un'operazione cosiddetta di *hashing* a senso unico, con algoritmo di classe MD5, che genera un'impronta della lunghezza di 128 bit (16 byte).

³⁰ Su questo tipo di problemi in relazione al tema qui in discussione si v. G. DI PAOLO, *vc. La prova digitale*, cit.

³¹ A. GHILDARDINI, G. FAGGIOLI, *Computer Forensic*, cit., p. 54.

³² *Ibidem*, p. 55.

³³ G. COSTABILE, *Scena criminis*, cit., p. 3.

L'impronta costituisce un riferimento certo alla traccia digitale, ma non ne consente una ricostruzione. Tale algoritmo è utilizzato a livello internazionale e garantisce un buon livello di sicurezza»³⁴.

Tuttavia, come ricordavamo, il processo penale è regolato dal principio del contraddittorio nella formazione della prova, e questo implica fra il resto che essa debba subire il vaglio della dialettica processuale: sembra pertanto legittimo chiedersi che cosa significhi "buon livello di sicurezza" e se, effettivamente, la procedura appena descritta possa essere accettata senza difficoltà.

§5. ...secondo la prospettiva retorica.

Ebbene, per quanto la procedura della creazione del c.d. "marchio digitale" sia garantita da sistemi utilizzati a livello internazionale, non mancano problemi di tipo informatico e critiche che incidono proprio sul valore processuale di quei procedimenti di ricerca della prova.

Per quanto attiene il primo profilo, si ricordi che

«una funzione di hash è una funzione matematica non invertibile in grado di processare un dato arbitrariamente grande e di calcolare, da questo, un valore di grandezza finita. È implicito in questa definizione che qualunque funzione di hash al mondo ha un problema evidente: essendo il numero di dati possibili infinito ed essendo, nel contempo, il numero risultante di grandezza fissa (quindi invariabilmente un numero finito di valori) esiste la probabilità che più dati diversi generino uno stesso valore di hash. Tale problema è noto come *collision*»³⁵:

e poiché si parla di "probabilità" il suo verificarsi è tutt'altro che meramente possibile ed esiste anzi la concreta evenienza che gli algoritmi più utilizzati nel campo della *computer forensic science* abbiano subito questo tipo di problema. Come si intuisce ciò è esattamente quello che è successo e sono stati trovati sistemi per generare in essi delle collisioni; ma non è tutto: infatti «è evidente come, con il crescere della potenza di calcolo fornita dai moderni calcolatori, sia sempre più semplice riuscire a trovare dei sistemi per generare collisioni e sia sempre più

³⁴ Loc. ult. cit. L'algoritmo MD5 è, insieme a SHA-1, il più utilizzato per la validazione della *legal imaging* [cfr. A. GHILDARDINI, G. FAGGIOLI, *Computer Forensic*, cit., p. 57].

³⁵ Loc. ult. cit.

complesso riuscire a sviluppare algoritmi che possa fornire una validazione per lungo tempo»³⁶.

Tutto questo rappresenta un importante problema per la garanzia di sicurezza dei sistemi di validazione perché il loro fine dovrebbe essere proprio quello di assicurare l'univocità del dato e l'impossibilità che esso possa venire generato da un altro sistema: impedire, cioè, che si produca una falsa *legal imaging* che risulterebbe però certificata dallo stesso valore di *hash* di quella autentica. I programmi usati per generare le funzioni di *hash* dovrebbero in effetti rendere impossibile predeterminare il verificarsi di una condizione di collisione: in caso contrario l'operazione di validazione perderebbe letteralmente di senso perché «sarebbe possibile variare *ad hoc* il dato valicato e calcolare poi la condizione necessaria per generare la *collision* con il valore calcolato sul dato originale. Si avrebbe quindi un dato modificato che però risulta identico all'originale all'applicazione della validazione»³⁷.

Si tratta, come ben si vede, di un problema essenzialmente informatico-matematico che richiede una soluzione di tipo informatico, come validare contemporaneamente il dato con due algoritmi, cosa che «rende praticamente impossibile calcolare una *collision* che sia valida al contempo per entrambi gli *hash*»³⁸.

Ma questo problema non è l'unico: ne esiste un altro, sempre di natura informatica, che però emerge con riferimento al diritto (e più esattamente al processo) e la cui soluzione, per quanto informatica, deve essere dettata da ragioni non tecniche. Si ricordi a tal proposito che per effettuare la copia 1 : 1 di un supporto digitale si possono usare *software* specializzati³⁹, che però sono protetti da *copyright* e quindi non danno la possibilità di conoscere il codice-sorgente del programma, che resta così nascosto anche agli esperti informatici nominati, in veste di consulenti, dalla difesa, dal pubblico ministero o dal giudice. Come è stato correttamente evidenziato, «si tratta [...] di una questione che merita la massima

³⁶ Loc. ult. cit.

³⁷ A. GHILARDINI, G. FAGGIOLI, *Computer Forensic*, cit., p. 58.

³⁸ Loc. ult. cit.

³⁹ Si pensi, ad esempio, al *software EnCase*, prodotto dalla *Guidance Software Inc.* che è «destinato all'uso professionale ed investigativo di numerose agenzie e forze dell'ordine in tutto il mondo e considerato in linea con gli standard internazionali per le analisi delle tracce informatiche» (G. COSTABILE, *Scena criminis*, cit., p. 7, nt. 3).

attenzione e che dovrà nel futuro essere oggetto di approfondimenti dottrinali»⁴⁰: ma come spesso accade, prima che questi siano condotti a termine la prassi cerca di fornire le proprie risposte.

Come si intuisce, infatti, l'utilizzo di quel tipo di sistemi potrebbe agevolare la presentazione di eccezioni in ordine alla legittimità della prova di cui si richiede l'acquisizione: e, in effetti, proprio per evitare possibili eccezioni della difesa – la quale potrebbe lamentare (secondo noi sensatamente) la mancata trasparenza della «procedura di *working* dell'analizzatore»⁴¹ e così impedire l'ingresso, all'interno del processo penale, di una prova digitale pregiudizievole per l'imputato –, «alcune squadre investigative si stanno orientando verso l'utilizzo di software a codice-sorgente aperti (*open source*)»⁴². In effetti, se non si è in grado di conoscere il codice-sorgente di un programma informatico non si è in grado di conoscere le istruzioni appartenenti al linguaggio di programmazione utilizzato per realizzare quel programma: qualcosa sul suo funzionamento (ma, verrebbe da dire, le ragioni intrinseche dello stesso) resterebbe così celato e nascosto.

Ma proprio come una dimostrazione condotta con il *computer* può non essere considerata valida in matematica, un argomento che per sua natura non si rende disponibile alla confutazione non può essere considerato legittimo in processo, dove solo ciò che può essere discusso può trovare autenticamente spazio⁴³. Cosa che, invece, non sarebbe allo stato possibile ove si chieda l'acquisizione di una prova digitale, poiché la procedura informatica seguita nella ricerca della prova medesima non risulterebbe controllabile in ogni sua parte: il programma con cui si ottiene la certificazione dell'autenticità della *legal imaging* dei dati analizzati, proprio perché coperto da *copyright*, non può infatti essere letto. Allo stato, quindi, «non essendo possibile analizzare i codici-sorgente di questi programmi, la validità dei *report* da loro generati è fondata su un vero e proprio atto di fede»⁴⁴: e questo è inaccettabile nel contesto di un processo che pretende di essere razionale e che, solo nella misura in cui lo sia, può essere controllato.

⁴⁰ L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali*, «Diritto dell'internet», n. 2, 2006, p. 155-160: 158, nt. 26.

⁴¹ G. COSTABILE, *Scena criminis*, cit., p. 7, nt. 3.

⁴² L. LUPARIA, *Il caso "Vierika"*, cit., p. 158, nt. 26.

⁴³ Cfr. i saggi contenuti in M. MANZIN, F. PUPPO (a cura di), *Audiatur et altera pars*, cit.

⁴⁴ A. MONTI, *Attendibilità dei sistemi di computer forensic*, «ICT-Security», 9, 2003 (disponibile on line: <<http://www.ictlex.net/?p=287>>. Accesso il 28 ottobre 2012), p. 2.

Non potendo “entrare” nel sistema, ci sembra così che la giustificazione idonea a fondare l’uso processuale di quei *software* resterebbe che questi vengono comunemente utilizzati: ma evidentemente non si può certo basare la legittimità dell’utilizzo di alcunché sul fatto che questo viene utilizzato. Viceversa, nulla si potrebbe obiettare, neppure in sede di eccezione processuale, se fosse possibile accedere ai codici-sorgenti dei programmi di *legal imaging* perché un tanto basterebbe a rendere del tutto disponibile alla controparte ogni passo del metodo tramite il quale si è pervenuti alla prova digitale. Si tratta di un risultato che, peraltro, potrebbe essere ottenuto in modo piuttosto semplice, utilizzando un comando del sistema operativo Unix, e cioè «Unix dd. Si tratta di un tool [...] di copia sequenziale utilizzato sotto Unix per scopi di vario genere»⁴⁵ che consente, fra molti vantaggi di tipo tecnico-informatico, anche quello «di essere disponibile, insieme ad alcuni interi sistemi operativi Unix-like (come GNU/Linux, Darwin, e i vari *BSD), in formato sorgente. Ciò implica che a qualunque eccezione posta in fase di dibattimento sull’effettivo funzionamento del software è possibile rispondere sia mostrando il codice sorgente sia ricompilandone una nuova versione per mostrarne l’effettivo funzionamento»⁴⁶.

E in questo modo – ma ci verrebbe da dire: solo in tal modo – potrebbe appieno spiegarsi il principio del contraddittorio che garantisce lo svolgersi del giusto processo, essendone ad un tempo principio logico, ontologico e deontologico⁴⁷. Chi sottace o non è in grado di mostrare alla controparte le ragioni del proprio dire, infatti, si sottrae al dialogo, comportandosi in modo eticamente scorretto, in un processo che sarà di conseguenza ingiusto: e non essendo un giusto processo, esso non potrà neppure essere considerato un vero processo.

§6. Conclusioni.

In tal modo auspichiamo di avere chiarito la natura del nesso che prima abbiamo annunciato fra dimostrazione matematica e argomentazione processuale: in effetti, se un teorema matematico non può essere pacificamente accettato ove

⁴⁵ A. GHILARDINI, G. FAGGIOLI, *Computer Forensic*, cit., p. 59.

⁴⁶ Loc. ult. cit.

⁴⁷ Cfr. M. MANZIN, Del contraddittorio come *principio* e come *metodo*, cit.; ID., *Avvocati custodi del processo: alle radici della deontologia forense*, in M. MANZIN, P. MORO (a cura di), *Retorica e deontologia forense*, Milano: Giuffrè, 2010, pp. 3-18.

non sia possibile seguirne passo passo la dimostrazione, ci pare che, a maggior ragione, non possa essere accettata un'argomentazione la quale si sviluppi nel contesto controversiale del processo ma senza potere essere inserita nel contraddittorio.

Da quanto detto, emerge peraltro una singolare simmetria: sia la dimostrazione del teorema dei quattro colori, sia l'autenticità della *legal imaging* possano essere accettate solo se si è *convinti* che i programmi rispettivamente impiegati eseguano ciò che i loro autori affermano. Ma, nell'esempio della prova digitale, se non si conoscono i codici-sorgenti dei programmi utilizzati, ciò non può succedere: a meno, come cennato, di non far ricorso ad un argomento *ex auctoritate*, qual è quello dell'efficacia, che ricorda molto da vicino la visione moderna del diritto simboleggiata dal motto hobbesiano *auctoritas non veritas facit legem*, la cui filosofia di impronta positivista ha segnato la nascita stessa dell'informatica giuridica.

Oggi, però, le cose si presentano in modo più complesso, soprattutto ove si guardi all'incidenza degli strumenti informatici sul diritto nel suo farsi concreto e sulle reciproche influenze che l'informatica ed il diritto esercitano l'una sull'altro⁴⁸: ciò consente, peraltro, di recuperare, in senso non più divisionista, il dibattito sulla natura del sapere scientifico e del sapere giuridico, in nome di un pluralismo metodologico⁴⁹ ma anche logico⁵⁰.

⁴⁸ Per un approfondimento del punto ci sia consentito rimandare al nostro F. PUPPO, *Informatica giuridica e metodo retorico*, cit.

⁴⁹ Tesi sviluppata, su tutti, da Vittorio Villa, in primo luogo e sin dal suo V. VILLA, *Teorie della scienza giuridica e teorie delle scienze naturali. Modelli e analogie*, Milano: Giuffrè, 1984.

⁵⁰ Per un primo esame del quale ci sia consentito rimandare al nostro F. PUPPO, *Metodo, pluralismo, diritto. La scienza giuridica tra tendenza 'conservatrici' e 'innovatrici'*, Roma: Aracne, 2013 (in part. pp. 171ss), oltre che alle indicazioni bibliografiche ivi contenute