Editoriale | *Editorial*

SERGIO LORUSSO

Professore ordinario di Diritto processuale penale – Università degli Studi di Foggia

Digital evidence, cybercrime e giustizia penale 2.0
Digital evidence, cybercrime and criminal justice 2.0

La rivoluzione digitale ha inciso profondamente sul processo penale e, in particolare, sull'orizzonte probatorio. Alla base, la possibilità di fruire di strumenti d'accertamento di grande efficacia ma, al contempo, di inconsueta invasività. Affrontare le numerose questioni che il "nuovo mondo" tecnologico suscita significa approcciarsi in maniera bilanciata al tema delle sinergie tra universi apparentemente inconciliabili. L'*iter* di adeguamento del nostro ordinamento alla nuova realtà è stato caratterizzato da ritardi e da scarsa consapevolezza delle peculiarità del fenomeno, che hanno prodotto adattamenti forzati di istituti tradizionali e supplenze (talora divenute derive) giurisprudenziali, nonostante gli inputs sovranazionali che – specie di recente – hanno mostrato di comprendere l'irrinunciabilità di una regolamentazione *ad hoc* della *digital evidence*, vero e proprio archetipo della "prova globale" che costituisce un dato fondante della giustizia penale 2.0. Da qui la necessità di un mutamento di prospettiva, di un cambio di passo che riconosca le ricadute in ambito processuale della società digitale, pervasiva ormai di ogni aspetto della vita quotidiana del terzo millennio.

The impact of digital revolution on criminal justice is strong, in particular on law of evidence. Basically, the chance to use investigation tools which are very effective but, at the same time, dangerously intrusive. Facing the numerous questions that the technological "new world" raises means approaching in a balanced way to the issue of synergies between apparently irreconcilable universes. The process of adapting the existing rules to the new reality was characterized by delays and scarce awareness of the issue, which have produced forced adaptations of traditional institutions and confused case law, despite the supranational inputs that – especially recently – have shown to understand the indispensability of a specific regulation of digital evidence, a true archetype of the "global evidence" which characterizes the criminal justice system 2.0. Hence the need for a change of perspective, to understand the impact of digital society on criminal justice.

«Computers are incredibly fast, accurate and stupid;
humans are incredibly slow, inaccurate and brilliant; together they are powerful beyond imagination»

UOMINI E MACCHINE DI FRONTE ALLA GIUSTIZIA PENALE

"I computer sono incredibilmente veloci, precisi e stupidi; gli esseri umani sono incredibilmente lenti, imprecisi e brillanti; insieme sono potenti oltre l'immaginazione": l'affermazione, tradizionalmente (ed erroneamente) attribuita ad Albert Einstein ma presumibilmente ascrivibile all'economista statunitense Leo Cherne, può costituire un valido punto di partenza per affrontare la tematica delle interazioni tra rivoluzione digitale e sistema penale, nelle sue declinazioni sostanziali e processuali.

L'irruzione dell'universo informatico nella realtà quotidiana, difatti, ha determinato – al contempo – ricadute nel catalogo delle fattispecie penali (ampliandolo talora nel senso della specificazione di figure di reato esistenti e in altri casi originando nuove fattispecie in precedenza neanche ipotizzabili perché legate all'innovazione tecnologica) e riverberi nell'orizzonte probatorio, fornendo strumenti d'accertamento dall'inusitata efficacia ma dall'altrettanto inedita e non facilmente governabile invasività. Con tutto quello che ne consegue in termini di tutela (effettiva) delle garanzie individuali, presidio irrinunciabile almeno fino a che le stesse continueranno ad essere il perno attorno al quale gira il sistema giu-

stizia in ragione della sua vocazione liberale.

La citazione iniziale fornisce, o dovrebbe fornire, la traccia corretta – sotto il profilo concettuale e gnoseologico, prima ancora che giuridico – per affrontare e risolvere le delicate questioni che il "nuovo mondo" ad alto tasso tecnologico (e fortemente orientato verso la tecnocrazia) inevitabilmente pone. Perché le norme, com'è noto, non sono delle monadi, non vivono in maniera indipendente rispetto al contesto (sociale, politico e culturale) che le esprime. Anche in un'ipotetica società del futuro dominata da macchine create dall'uomo le regole rifletterebbero la *Weltanschauung* condivisa (liberamente o forzatamente) dal relativo gruppo sociale, magari elaborata da un sistema binario sulla base di *bit*.

Da qui la necessità di fondere le peculiarità e le inclinazioni (verrebbe da dire, i talenti) di due universi apparentemente inconciliabili per trarne un valore aggiunto, quell'*upgrade* che potrebbe – e dovrebbe – fornire agli ingranaggi processuali strumenti in grado di migliorarne il funzionamento, senza per questo relegare nell'angolo il repertorio dei diritti e delle garanzie plasticamente scolpiti nella Carta fondamentale.

A patto, naturalmente, di non snaturare l'essenza dei singoli (e assai diversi) mondi né di oscurare l'inevitabile ed indiscutibile primato dell'uomo sulle macchine e – nello specifico – del diritto sulla scienza, che del primo – nell'area della giustizia penale – può essere un'ancella e non certo un *comodus discessus* per sottrarsi agli oneri che fanno capo al giurista e alle responsabilità di cui l'apparato giudiziario è investito proprio dal patto sociale.

Dell'esperienza digitale si sottolinea la velocità di calcolo e la precisione, certamente non eguagliabili da parte degli esseri umani, ritenuti però brillanti, creativi e intuitivi. L'ultima frontiera, com'è noto, è quella dell'intelligenza artificiale[1]: fronte della ricerca attraverso cui si intende emancipare i *pc* dalla loro tradizionale "stupidità" per promuoverli a macchine pensanti in grado di affiancare, se non di superare, l'uomo. Il tutto, però, sempre sulla base di algoritmi che costituiscono la linfa (esclusiva) con cui si alimenta la sfera digitale. Ne scaturiscono temi e problematiche che investono non soltanto il terreno tecnico-scientifico ma anche la dimensione etica della conoscenza e dell'agire umani. Il sistema digitale è governato dai numeri ed è manipolabile, senza che spesso si sappia da chi (e perché); l'uomo è corruttibile, ma risponde comunque in prima persona ed ogni azione è riferibile ad un soggetto determinato.

L'irrompere sulla scena dell'intelligenza artificiale, a sua volta, amplifica tali tematiche, esaltandone l'azzardo, nella prospettiva di un futuro – magari meno remoto di quanto oggi si possa immaginare e prevedere – nel quale la sostanziale equiparazione tra uomo e macchina delle rispettive potenzialità possa porre la questione del predominio dell'uno sull'altro. E, magari, far materializzare scenari finora esclusivo appannaggio della letteratura distopica e della cinematografia ispirata alla *science fiction* nei quali computer e replicanti dall'anima digitale binaria conquistino il potere sull'umanità riducendola in schiavitù.

Colpevoli ritardi e incertezze normative

L'era digitale esiste.

Ormai è una realtà, che si riverbera su ogni segmento della vita quotidiana, ed ignorarla sarebbe un errore. Occorre quindi collocarla in un contesto adeguato, che non stravolga l'essenza della giurisdizione. In questo, per la verità, il legislatore italiano raramente ha operato con tempestività, procedendo "a traino" e spesso solo quando necessitato dagli *inputs* di derivazione sovranazionale. Non regolamentare equivale a lasciar spazio a prassi devianti o ad improbabili letture giudiziarie più o meno marcatamente estensive della normativa vigente, piegata ad un adattamento forzato e spesso inadeguato imposto proprio dall'immobilismo del legislatore.

Paradigmatica è la vicenda relativa al captatore informatico, che solo con il d.lgs. 29 dicembre 2017, n. 216, peraltro soggetto a un ininterrotto flusso normativo procrastinatore tuttora in corso, ha ottenuto un riconoscimento legislativo, non senza falle e deboli soluzioni foriere di dubbi e incertezze, che quantomeno – però – ha segnato i confini entro cui è possibile avvalersi di uno strumento investigativo tanto efficace quanto invasivo e in grado di frantumare la sfera personale di privatezza, fornendone al con-

[1] Il tema, in realtà, è tutt'altro che nuovo, essendo stato scandagliato anche in Italia già sul finire del secolo scorso: si veda, in particolare, G. Sartor, *Intelligenza artificiale e diritto. Un'introduzione*, Milano, Giuffrè, 1996, *passim*.

tempo un adeguato – pur se non del tutto soddisfacente – inquadramento sistematico [2] che supera la lettura giurisprudenziale secondo cui la captazione informatica altro non sarebbe se non un'"intercettazione ambientale itinerante" [3] e dunque, in sostanza, un'intercettazione atipica priva di una sua autonomia concettuale.

Centrale, in questo ambito, è l'*iter* di ratifica della Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001, perfezionato con la l. 18 marzo 2008, n. 48 [4] (e dunque a distanza di oltre sette anni). Una Convenzione che, com'è noto, ha esplorato e regolamentato per la prima volta – tracciandone le coordinate fondamentali e scandendo così una *road map* indirizzata ai singoli ordinamenti nazionali – l'area dell'impiego *contra legem* dei sistemi informatici (nelle loro componenti *hardware* e/o *software*), quale fonte di illeciti penali, unitamente all'utilizzazione in chiave investigativa e probatoria delle tecnologie informatiche.

Quest'ultimo profilo si è andato a posizionare in un ambito segnato da un'ampia produzione giurisprudenziale, proliferata – come ricordato – a causa di una perdurante stasi legislativa, risoltasi peraltro con soluzioni normative poco coraggiose e alquanto adagiate sull'esistente. Scelte che, sul piano sistematico (e non solo), si sono tradotte in "sotto-istituti" dotati di scarsa autonomia e, dunque, in figure prive di una loro pregnante identità, come invece la peculiarità e l'unicità della materia avrebbero richiesto.

Ispezioni, perquisizioni, sequestri, intercettazioni di comunicazioni: categorie tradizionali, collocate in un preciso e rigoroso recinto, sono state piegate per comodità, pigrizia e superficialità dei *conditores* – ma forse anche per una mancata (o quantomeno insufficiente) consapevolezza della novità e della rilevanza del fenomeno da normare – allo scopo di regolamentare strumenti investigativi e probatori la cui specificità, quanto meno in ragione delle caratteristiche esclusive del dato informatico (a partire dalla sua natura immateriale), avrebbe imposto una normativa anche concettualmente *ad hoc* in grado di assorbire i connotati di tali fonti di prova e di restituirli sotto forma di coerente architettura normativa [5].

Evitando di far insorgere problematiche e di far emergere criticità probabilmente prevedibili, a partire dalla fase investigativa [6] – ove la maggiore fluidità del dato probatorio comporta fatalmente un maggior grado d'incidenza sui diritti fondamentali dei soggetti coinvolti, sia in chiave processuale che extraprocessuale – per giungere a quella dibattimentale, dove la dote ricevuta dal precedente stadio procedimentale è di per sé ricca di un patrimonio probatorio digitale, per sua natura formatosi in assenza di contraddittorio, spendibile per la decisione finale. Avrebbero dovuto essere sufficienti queste considerazioni a suggerire maggiore attenzione ed oculatezza ad un legislatore che, invece, sembra sia stato colto di sorpresa dalla tempesta digitale.

Eppure l'interrelazione tra il mondo informatico e la giustizia penale non è comparsa all'improvviso, come un fulmine in una mattina di sole, se è vero che già nel 1989 il Consiglio d'Europa dettò delle *Raccomandazioni sulla criminalità informatica* [7] dedicate proprio al *Cybercrime*, nelle quali le relative ipotesi di reato erano suddivise in liste, la prima delle quali conteneva le condotte "minime" rispetto a cui i singoli Stati non avrebbero dovuto esimersi dal prevedere l'incriminazione, a differenza della seconda nella quale rientravano una serie di comportamenti per i quali vi era un mero suggerimento a ricondurli nell'alveo degli illeciti penali. Si era agli albori della rivoluzione informatica, eppure si avvertiva già come pressante l'esigenza di reprimere condotte illecite rispetto alle quali, evidentemente, le tradizionali fattispecie non

[2] Prospettiva condivisa da M. Bontempelli, *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont.* online, 2018, pp. 1-2, nel quadro di una più ampia riflessione tesa a far emergere i limiti della regolamentazione del captatore informatico indotta dalla "legge Orlando".

[3] Cass., sez. un., 28 aprile 2016, n. 26889, in *Dir. pen. cont.* online, 7 ottobre 2016, con nota di G. Lasagni, *L'uso di captatori informatici (*trojans*) nelle intercettazioni "fra presenti"*, *ivi*.

[4] Per un'analisi globale dei contenuti della legge con cui il nostro ordinamento ha recepito la Convenzione di Budapest si rinvia ad AA.VV., *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul* cybercrime *(L. 18 marzo 2008, n. 48)*, a cura di L. Lupária, Milano, Giuffrè, 2009, *passim*.

[5] Sulla stessa lunghezza d'onda le considerazioni di S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, Giappichelli, 2018, p. 3, che evidenzia il verificarsi di «uno stravolgimento degli impianti sistematici e della logica in cui sinora si è mossa la stessa costruzione teorica della materia, oltre che l'approccio concreto che ne è derivato».

[6] Si vedano le riflessioni svolte da E. Lorenzetto, *Le attività urgenti di investigazione informatica e telematica*, in AA.VV., *Sistema penale e criminalità informatica*, cit., p. 135 s.

[7] Raccomandazione n. R (89) 9 del 13 settembre 1989 da parte del Comitato dei Ministri del Consiglio d'Europa.

potevano essere sufficienti e adeguate. I riverberi processuali sarebbero venuti successivamente.

Ma che il nostro legislatore si sia trovato impreparato oltre un decennio più tardi, quando la cultura digitale era ormai diventata una realtà, è sintomatico di come, da troppo tempo, chi si occupa della cosa pubblica sia attratto dalle contingenze e dai provvedimenti "ad effetto" piuttosto che coltivare un serio e responsabile atteggiamento teso a realizzare architetture normative quanto più possibile in grado di tutelare i cittadini e gli interessi comuni contestualizzandoli nel presente per far crescere, migliorandolo, l'impianto giuridico complessivo che della società è l'architrave[8]. E tale atteggiamento di "estraneità" rispetto alla tematica risulta essere persistente anche nei più recenti approdi normativi in tema di *trojan* prima richiamati, con una pervicacia che suscita da più parti interrogativi di non facile soluzione[9]. Attraversare il *mare magnum* digitale, viceversa, impone la conoscenza di dati metagiuridici[10] senza dei quali un'adeguata lettura del fenomeno, funzionale alla sua regolamentazione, è pressoché impossibile e comunque foriera di fallacie e approssimazioni.

Digital evidence tra novità e criticità

Digital evidence è espressione – largamente condivisa a livello internazionale[11] – con la quale si racchiude all'interno di un'area omogenea l'insieme degli strumenti investigativi e probatori suscitati e alimentati dalla rivoluzione informatica. L'oggetto di prova (o di indagine), difatti, è indissolubilmente legato al mondo virtuale, non potrebbe esistere senza di esso, dal quale è stato generato e nel quale trova ospitalità.

Si tratta, peraltro, della prima area probatoria in assoluto nata e consolidatasi in un ambito sovranazionale: è la stessa impalpabilità della *digital evidence*, insieme all'assenza di coordinate spaziali – il suo formarsi in un "non-luogo" qual è il cyberspazio[12] – che contraddistingue il dato digitale ad aver imposto *ab initio* tale evoluzione (la mancanza di fisicità comporta giocoforza la necessità di superare i confini dei singoli Stati), consentendo presumibilmente a siffatta categoria di assurgere storicamente ad archetipo della "prova globale" destinata a contrassegnare il terzo millennio, diventandone il simbolo, così come in passato è accaduto, ad es., per la confessione e per la testimonianza, considerate le "prove regine" in un mondo nel quale l'uomo e la sua corporeità erano al centro della vita quotidiana[13]. Non è un caso che la tortura, degenerazione della prova dichiarativa in auge nel Medioevo, facesse leva sui corpi – dai quali si voleva "estrarre" l'anima dell'inquisito – per ottenerne risultati probatori.

Vi è anzi chi, in maniera estrema, profetizza una "dittatura" prossima ventura della *digital evidence*, un'epoca in cui assisteremo al monopolio delle fonti di prova digitali[14]. Scenario futuribile o improbabi-

[8] Significativo, viceversa, è l'intuito – non solo giuridico – di chi è stato precursore nella percezione della rilevanza che tale ambito avrebbe assunto, proponendo una riflessione di taglio interdisciplinare: L. Lupária-G. Ziccardi, *Investigazione penale e tecnologia informatica*, Milano, Giuffrè, 2007, *passim*.

[9] G. Giostra-R. Orlandi, *Introduzione*, in AA.VV., N*uove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di G. Giostra e R. Orlandi, Torino, Giappichelli 2018, p. XI, sottolineano come non sia «facile capire il senso di questa riluttanza del legislatore ad affrontare i molteplici problemi di informatica forense, con l'ampiezza che avrebbe imposto la concreta applicazione delle nuove tecnologie all'indagine penale».

[10] V., in proposito, le incisive ed esaurienti riflessioni di S. Signorato, *Le indagini digitali*, cit., p. 9 s.

[11] Per considerazioni lessicali sul ventaglio di formule adottate per descrivere il fenomeno e sulle ricadute definitorie, classificatorie e sistematiche (gravide di conseguenze sul piano applicativo) si rinvia a M. Pittiruti, Digital evidence *e procedimento penale*, Torino, Giappichelli, 2017, p. 6 s.

In precedenza, relativamente al concetto di *computer forensics*, anche in chiave ricostruttiva della sua evoluzione storica, v. G. Ziccardi, *L'origine della* computer forensics *e le definizioni*, in L. Lupária-G. Ziccardi, *Investigazione penale e tecnologia informatica*, cit., p. 31 s.

[12] In questa direzione A. Ingrassia, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine? Le responsabilità penali dei* provider *nell'ordinamento italiano*, in AA.VV., Internet provider *e giustizia penale*, a cura di L. Lupária, Milano, Giuffrè, 2012, p. 16 e 18-19.

[13] L. Luparia, *La disciplina processuale e le garanzie difensive*, in L. Lupária-G. Ziccardi, *Investigazione penale e tecnologia informatica*, cit., p. 127, lucidamente osserva come «le svolte epocali che lungo i secoli hanno interessato il rito penale assai di rado [siano] state registrate dagli interpreti del periodo con sollecitudine e immediatezza, giacché il vincolo della contemporaneità ha molte volte impedito di annotare tempestivamente le profonde trasformazioni che andavano producendosi».

[14] G. Ziccardi, *Informatica giuridica.* Privacy, *sicurezza informatica,* computer forensics *e investigazioni digitali*, vol. II, Milano,

le vaticinio? Sarà il tempo a dircelo, ma è certo che se pensiamo alla travolgente e inarrestabile corsa di cui è stato protagonista il mondo digitale, che ha finito per affiancarsi e fondersi con la realtà preesistente dando vita a un "mondo nuovo" fino a qualche decennio fa del tutto inimmaginabile, non possiamo ridurre a mere elucubrazioni le argomentate riflessioni di chi prova a vedere in proiezione gli assetti sociali derivanti dalla pervasività del fenomeno digitale – a partire dall'evoluzione del *web* 2.0 in *web* 3.0 – per coglierne le implicazioni sul piano processuale e in ispecie probatorio che di tali assetti sono il prodotto.

Ferme restando le specificità e l'autonomia di ciascun sistema processuale nazionale, la cui sovranità risulta ad oggi non essere messa in discussione nel pianeta della giustizia penale, una "prova globale" richiederebbe una regolamentazione universale che superi gli angusti limiti territoriali di ogni Stato e, comunque, è indubbio che la singolarità del *medium* pone proprio in materia probatoria una serie di problematiche inedite e di non facile risoluzione che dovranno inevitabilmente essere sviscerate.

Si pensi alla difficoltà di procedere al sequestro di dati informatici riconducibili a *server* operanti in altri Paesi, o gestiti a livello planetario in maniera impermeabile ad ogni ingresso non autorizzato, com'è accaduto nel caso della *Apple* per l'*iPhone* – il cui sistema "chiuso" impedisce ogni accesso – negli Stati Uniti d'America (2016), quando l'FBI ha chiesto all'azienda di Cupertino di accedere ai dati contenuti nel cellulare di un terrorista coinvolto nella strage di San Bernardino (2015) tramite una porta di accesso in grado di bypassare le tecniche di cifratura utilizzate da ogni *device* Apple a tutela della *privacy* dell'utente. Il telefono, infatti, era protetto da un codice pin a quattro cifre ed impostato per il *wiping* dei dati dopo dieci tentativi di inserimento errato del codice di blocco. La Apple rifiutò di fornire un apposito *software* di sblocco, adducendo ragioni di sicurezza e di protezione della sfera di riservatezza dei clienti, fiore all'occhiello delle sue politiche commerciali. Condotta innanzi al giudice che avrebbe dovuto dirimere la delicata questione, si trovò di fronte ad una richiesta di proroga formulata dall'FBI che affermò di aver trovato una terza parte in grado di sbloccare l'*iPhone* sequestrato. Qualche giorno più tardi l'FBI ritirò la richiesta presentata nei confronti della Apple, essendo riuscita ad ottenere lo sblocco del *device* e recuperato i dati aventi interesse investigativo.

Anche in Italia non mancano risvolti interpretativi legati alla penetrazione delle nuove tecnologie nel terreno ormai consolidato delle intercettazioni di comunicazioni (e, più in generale, delle captazioni di flussi verbali e telematici): più volte, infatti, la Corte di cassazione è intervenuta sul tema dell'acquisizione e dell'utilizzabilità di flussi di testo (c.d. *chat pin to pin*) scambiati tra soggetti mediante dispositivi *Blackberry* o applicazioni di messaggistica del tipo di *WhatsApp*, affermando che non è necessario ricorrere alla rogatoria internazionale poiché le comunicazioni avvengono in Italia, ritenendo ininfluente la circostanza che per decriptare i dati identificativi dell'utente occorra avvalersi della collaborazione del produttore del sistema operativo avente sede all'estero [15], e asserendo che sono utilizzabili le intercettazioni di *chat* protette da servizio *pin to pin* gestito da *server* situato all'estero (*WhatsApp*) senza avvalersi della rogatoria internazionale, proprio perché si tratta di dati registrati in Italia da impianti ubicati presso l'autorità giudiziaria (trasmessi dal gestore sulla memoria informatica di quest'ultimi) e, comunque, scambiati sul nostro territorio [16].

In realtà tale lettura è tutt'altro che pacifica. Com'è stato opportunamente osservato, infatti, un siffatto approccio non tiene conto – anche per evidenti ragioni di semplificazione dell'*iter* procedimentale – delle specificità degli strumenti oggetto di captazione, che si riverberano sulle modalità esecutive delle operazioni certo non sovrapponibili a quelle tradizionali [17]. Le ricadute in tema di rispetto delle garan-

Giuffrè, 2012, p. 296.

Di "processo informatico", non più assimilabile a un rito esoterico, parla A. Testaguzza, Digital forensics. *Informatica giuridica e processo penale*, Padova, Cedam, 2015, p. IX.

[15] Così, con riferimento all'acquisizione di messaggi veicolati via *Blackberry*, Cass., sez. IV, 8 aprile 2016, n. 16670, in *C.E.D.* Cass., n. 266983.

Nella stessa direzione, in precedenza, Cass., sez. VI, 22 settembre 2015, n. 39449, in *Arch. pen.* web, 2016, 1, con nota critica di L. Filippi, *Questioni nuove in tema di intercettazioni*: quid iuris *sul* "pin to pin" *dei* blackberry? *ivi*.

Senza dire, poi, dell'orientamento giurisprudenziale che ritiene riconducibile al *genus* prova documentale i dati delle *chat WhatsApp*: v., tra le tante, Cass., sez. V, 21 novembre 2017, n. 1822, in *www.diritto24.ilsole24ore.com*.

[16] Cass., sez. IV, 12 dicembre 2017, n. 32146, *inedita*.

[17] V., in proposito, S. Furfaro, *Le intercettazioni* "pin to pin" *del sistema* blackberry, *ovvero: quando il vizio di informazione tecnica porta a conclusioni equivoche*, in *Arch. pen.* web, 2016, 1; G. Pittelli-F. Costarella, *Ancora in tema di* chat "pin to pin" *su sistema telefonico*

zie difensive in ambito probatorio sono evidenti. Considerazioni dello stesso tenore valgono per l'intercettazione di comunicazioni effettuate via *Skype* [18].

Efficacia delle investigazioni, rispetto della *privacy*, sorveglianza e sicurezza pubblica convergono in un *mix* dal quale è davvero arduo trarre una visione unitaria che soddisfi interessi fortemente contrapposti, componendoli in un *unicum*, senza ridurli a mere icone.

Che si tratti di mezzi "potenti", in grado di imprimere alle investigazioni – prima – e alla compattezza della base cognitiva messa a disposizione dell'organo giudicante – poi – accelerazione e spessore rispetto a vicende giudiziarie anche complesse, magari destinate a rimanere sospese nel limbo o a essere risucchiate dalle sabbie mobili della prescrizione, è indubbio. Attualmente sarebbe difficile (se non impossibile) farne a meno, specie tenuto conto dei reati commessi in rete il cui accertamento è concretamente possibile soltanto avvalendosi di strumenti che sulla rete incidono. Come per le intercettazioni di conversazioni e di comunicazioni, diventate fino a qualche anno fa il canale privilegiato di indagine, e non solo per i reati associativi e per quelli contro la pubblica amministrazione, la nuova frontiera oggi è data proprio dalla *digital evidence*. Tale primato, peraltro, è simmetrico alla *leadership* che i supporti informatici hanno conquistato nella vita di tutti i giorni, che si muove ormai in maniera disinvolta tra realtà fisica e realtà virtuale (e che vede quest'ultima conquistare sempre maggiori spazi).

Da qui l'esigenza di un'azione legislativa che non travolga le garanzie difensive, a partire dal momento – in quest'ottica centrale – della ricerca delle fonti di prova. Ancora una volta si intersecano qui nel dato positivo e nel diritto vivente commistioni di istituti, regolamentazioni carenti e prassi devianti. L'urgenza di pervenire a risultati concreti non deve tradursi in un oscuramento dei diritti di coloro che sono coinvolti – a vario titolo – in un procedimento penale.

E come se, facendo leva sulla (presunta) maggiore idoneità della tortura sotto il profilo probatorio di far emergere materiali cognitivi affidabili ed efficaci, e magari decisivi ai fini della risoluzione del caso giudiziario, se ne proponesse la (re)introduzione, dimentichi della grave lesione della sfera personale e della dignità umana che essa comporta (a prescindere dalla sua valenza gnoseologica). Ma anche di come la sua maggiore affidabilità, un dogma nei tempi in cui se ne faceva uso (e abuso), sia tutta da dimostrare. Simmetricamente, pur nell'assoluta consapevolezza dello iato esistente tra le due tipologie probatorie, si potrebbe evidenziare la tutt'altro che pacifica infallibilità e superiorità della *digital evidence*: se il dato digitale è neutro, infatti, il suo essere trattato dall'uomo comporta possibili alterazioni, manomissioni, cancellazioni, deterioramenti e finanche soppressioni (volontarie o meno che siano), che ne inficiano la genuinità compromettendo irrimediabilmente l'esito delle indagini, magari indirizzandole in direzioni sbagliate con conseguenze irreparabili per i singoli.

Da qui l'importanza di concentrare l'attenzione sulla catena di custodia, in quanto il dato digitale deve essere conservato accuratamente e richiede mani esperte per evitare che la sua (teorica) alta affidabilità si traduca in una trappola cognitiva per il giudice, alimentata dall'aura di invincibilità che la circonda in ragione della sua vagheggiata oggettività, con evidenti riflessi in punto di diritto di difesa.

Ecco perché è fondamentale il tema – comune alle varie declinazioni della prova scientifica – dei protocolli da elaborare, adottare e applicare in queste circostanze: tema, per la verità, pressoché ignorato nel nostro ordinamento, di tal che la *Chain of Custody* rappresenta molto spesso il tallone d'Achille di tale strumento cognitivo, depotenziandone – al di là dei proclami – l'incidenza nell'accertamento giurisdizionale. Dolosa o colposa che sia, difatti, la manipolazione del dato digitale produce sfiducia nei confronti di una fonte di prova che si ammanta di un peso specifico assai elevato. Perché al legislatore sia sfuggita – e continui a sfuggire – l'importanza di tale profilo nell'economia complessiva della prova scientifica non è dato sapere.

Sull'altro fronte si pone la questione della protezione dei dati individuali e della riservatezza individuale rispetto a strumenti la cui "aggressività" rispetto alla sfera intima e personale di ciascuno è dirompente e si traduce in una sorta di Grande Fratello, in grado di controllare tutto e tutti: i già noti fenomeni di invasione tentacolare del terreno delle conversazioni e delle comunicazioni – che non di rado coinvolgono persone del tutto estranee agli ipotetici reati oggetto delle indagini, la cui intimità viene duramente violata per essere poi divulgata dai *media* – si riproducono in maniera esponenziale. *Smartphone*, *pc*, *tablet* ed *e-mail*, in fondo, non sono altro che la versione contemporanea del diario, in

BlackBerry, *ivi*, 2016, 1; M. Trogu, *Come si intercettano le* chat pin to pin *tra dispositivi* Blackberry?, in *questa Rivista*, 2016, 3, p. 73 s.

[18] Su tale profilo si rinvia a M. Trogu, *Le intercettazioni di comunicazioni a mezzo* Skype, in *questa Rivista*, 2014, 3, p. 102 s.

cui ciascuno un tempo annotava ciò che era accaduto nella giornata. Qualcosa di talmente coessenziale a ciascuno di noi, «una parte così pervasiva e insistente della vita quotidiana che il proverbiale visitatore di Marte potrebbe ritenere che si tratti di una caratteristica importante dell'anatomia umana»[19]. Un diario, però, di una precisione inaudita e millimetrica, che non scarta nulla riportando fotogramma per fotogramma la vita di ciascuno, e che – per questo – è paradossalmente meno attendibile del vecchio quaderno vergato a penna che della vita quotidiana riportava una sintesi ragionata. Ogni frammento può essere infatti estrapolato e, magari, interpretato in maniera fuorviante se scollegato dal contesto complessivo. Fenomeno già noto all'universo delle captazioni, ma che qui assume giocoforza una portata maggiore, risultando pericolosamente amplificato.

Il captatore informatico, attraverso l'installazione di un *malware* su un dispositivo elettronico remoto (fisso o mobile), consente di entrare nelle vite degli altri, raccogliendo non solo conversazioni vocali e digitali ma anche immagini statiche o in movimento della quotidianità, realizzando il grado massimo di intrusione nell'agire individuale. Quanto al *web*, è ambiente che stride con il diritto all'oblio, mettendo in quarantena il diritto alla reputazione di chi è stato coinvolto in un processo penale, e poi magari assolto o addirittura destinatario di un provvedimento di archiviazione. Oscurando, in definitiva, la piattaforma costituzionale che assicura ad ogni individuo la tutela della privatezza e che ruota intorno all'art. 15 comma 1 Cost. il quale, non a caso, definisce come inviolabili – a conferma dell'inderogabilità di tale valore nell'architettura voluta dai Padri costituenti – la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione.

Giustizia penale 2.0

Mutuando l'espressione dal linguaggio informatico, ed adattandola all'universo giuridico, è possibile oggi parlare di *Giustizia penale 2.0*.

Di una giustizia, cioè, scandita dalle ricadute normative e applicative – ma anche concettuali – della digitalizzazione della società. Se ne è fornito fin qui un quadro, seppur parziale (e sintetico), con riferimento alle dinamiche probatorie, sicuramente le più importanti (e delicate) all'interno del processo penale.

L'area d'incidenza del *web*, di internet e dell'apparato informatico in genere (nelle sue componenti *hardware* e *software*), difatti, è assai più ampia e contribuisce a creare una sorta di struttura processuale parallela, naturalmente con molteplici intersezioni con l'assetto tradizionale e priva (allo stato) di una sua autonomia: una struttura verosimilmente destinata ad avere un peso sempre maggiore nell'economia complessiva del processo penale. A risentirne potrebbero essere proprio i canoni costituzionali, forse destinati – se non ad essere sovvertiti – ad essere rimodellati.

Contribuisce a tale rivoluzione sottile il c.d. "processo penale telematico", divenuto oramai una realtà. Certo, si tratta del profilo meno destabilizzante, destinato ad incidere fondamentalmente sui profili ordinamentali, ma sintomatico di un apparato giudiziario sempre più orientato alla smaterializzazione (un po' come sta accadendo, progressivamente, nella quotidianità di ciascuno di noi). Emergono anche in questo ambito le differenze (culturali e) strutturali con altri rami della giurisdizione, ove l'*iter* di digitalizzazione risulta più avanzato, che rendono più ardua la realizzazione di un progetto teso a digitalizzare una serie di dati e di flussi informativi alcuni dei quali coperti da segreto. Naturalmente tale itinerario pone questioni di non poco conto in relazione alla possibilità di penetrare nei sistemi informatici che conservano e gestiscono tali dati da parte di *hacker* che attraverso *malware* mettano a repentaglio il diritto alla riservatezza dei titolari dei dati medesimi e gli esiti stessi dell'attività investigativa in ragione di possibili fughe di notizie.

In ambito sovranazionale, poi, emerge una precisa linea di tendenza tesa ad implementare l'utilizzo dei dati digitali, in particolare nell'ambito della lotta ai crimini transnazionali, a partire proprio dalla succitata Convenzione di Budapest in materia di *Cybercrime* che può essere considerata l'apripista di una trama futuribile caratterizzata dal superamento del c.d. "modello Westfalia" (1648) – emblema sto-

[19] La considerazione, tutt'altro che estemporanea e sopra le righe, è della Corte suprema degli Stati Uniti d'America che, nell'affermare la necessità di un mandato *ad hoc* (anche in caso di arresto) per procedere alla perquisizione di un telefonino, in una sentenza paradigmatica del 2014 relativa al IV Emendamento ha evidenziato come il novanta per cento degli americani lo possieda e che gli *smartphone* costituiscono «una parte pervasiva e onnipresente della vita quotidiana» contenente «una trascrizione digitale di ogni aspetto delle loro vite, dai più banali a più intimi» (Riley v. California, 573 U.S. _ (2014)).

ricamente indiscusso della nascita dello Stato assoluto e, dunque, di un riconoscimento "forte" della sovranità nazionale – e della quale si colgono tracce in ambito comunitario – non senza difficoltà di adeguamento alle peculiarità del dato cognitivo digitale – nella disciplina dell'ordine europeo di indagine penale (Direttiva 2014/41/UE, attuata nel nostro Paese dal d.lgs. 21 giugno 2017, n. 108).

Più recentemente, in maniera pregnante ed organica, la Commissione europea ha presentato una proposta di Regolamento tesa ad istituire due inediti ordini europei volti alla produzione (OPE) ed alla conservazione (OCE) delle prove digitali in materia penale (COM (2018) 225 *final*) ed una proposta di Direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali (COM (2018) 226 *final*)[20], da cui si evince la consapevolezza della crescente rilevanza della *e-evidence* e dell'urgenza di intervenire sul tema per evitare prassi approssimative – quando non improvvisate – spesso lesive dei diritti individuali.

La stessa elaborazione dottrinale, del resto, ha trovato nel *web* una collocazione naturale e sempre più prevalente rispetto al supporto cartaceo. Il fenomeno, com'è ovvio, non ha ricadute processuali ma è emblematico di un universo – anche giuridico – che ha virato inequivocabilmente verso un nuovo mondo, un'*archè* digitale.

Al "nuovo mondo" che si è aperto negli ultimi anni, in definitiva, non si possono chiudere le porte.

Occorrerà, invece, uno sforzo – si spera congiunto – degli studiosi, degli operatori e del legislatore che armonizzi la rivoluzione digitale con l'impianto processuale consolidato, nell'ottica – che non vuole apparire utopistica – di un umanesimo digitale (peraltro auspicabile in ogni ambito applicativo dell'informatica). Perché sicuramente assisteremo, nel medio-lungo periodo, ad un profondo e significativo mutamento di assetti oggi ritenuti intangibili.

Ai processualpenalisti il compito di non ammainare la bandiera di un processo garantito e di continuare ad agitare il vessillo dei diritti della persona (evitando però sterili contrapposizioni e rigide difese dell'esistente), che non devono essere scalfiti in nome di una giustizia digitale di sapore tecnocratico dimentica dell'uomo: sarebbe un paradosso, visto che è stato proprio l'uomo a creare l'universo digitale. Divenirne schiavo equivarrebbe evidentemente ad una beffa.

Ed allora, non si può che concludere con il pensiero di un filosofo cui tanto deve la scienza giuridica, Karl Popper, secondo il quale "solo il cervello umano può attribuire un senso alla cieca capacità dei calcolatori di produrre verità". Come dire, in definitiva, che le sinergie tra uomini e macchine sono benvenute e possono produrre risultati un tempo impensabili, arricchire la nostra vita e migliorare anche il funzionamento del sistema giustizia; a patto, però, che – anche in tempi di intelligenza artificiale – siano i primi a guidare il funzionamento delle seconde e non viceversa e, dunque, a fissare gli obiettivi e a dettare le linee di condotta di un'interazione che costituisce il dato caratterizzante del terzo millennio.

[20] In maniera esaustiva, sul punto, si veda M. Gialuz-J. Della Torre, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. cont.* online, 2018, 5, p. 1 s.