"Società del Controllo" e documentazione informatica: il problema della prova digitale

Autori: Costantini, Federico (Università degli Studi di Udine, Dipartimento di Scienze Giuridiche), De Stefani, Marco Alvise (Synaptic Srls)

Bio: Dott. Avv. **Federico Costantini**, Prof. Aggr. di informatica giuridica e Teoria generale del diritto Dipartimento di scienze giuridiche, Università degli Studi di Udine.
Laureato in Giurisprudenza presso l'Università degli Studi di Padova nel 2000, Dottore di ricerca in "Filosofia del diritto (Metodi e tradizioni giuridiche)" nel 2004, Avvocato abilitato presso la Corte d'Appello di Trieste e iscritto all'Ordine forense di Udine nel 2007, è ricercatore confermato in Informatica giuridica presso il Dipartimento di Scienze giuridiche dell'Università degli Studi di Udine dove è attualmente incaricato per i corsi di Informatica giuridica e Teoria generale del Diritto dopo essere stato per diversi anni "cultore della materia" in Filosofia del diritto, Informatica giuridica e Teoria dei diritti umani.
Nel 2012 è stato nominato componente della seconda sottocommissione per l'abilitazione all'esercizio della professione forense presso la Corte d'Appello di Trieste su designazione del Dipartimento di Scienze giuridiche dell'Università degli Studi di Udine.
I suoi interessi gravitano principalmente ai problemi giuridici che emergono in relazione a tre temi: I sistemi "peer to peer" nella "sharing economy", il trattamento e la condivisione della prova informatica, la sicurezza nell'applicazione dell'intelligenza artificiale nell'ambito degli "autonomous vehicles".
Su tali argomenti in particolare ha scritto diversi articoli e contributi pubblicati in Italia e all'estero.
Attualmente è impegnato nella partecipazione all'iniziativa "Wider Impacts and Scenario Evaluation of Autonomous and Connected Transport", programma di ricerca COST, e nell'organizzazione della Clinica di Informatica giuridica, laboratorio finanziato come iniziativa di "didattica innovativa" dall'Ateneo udinese.
Per ulteriori informazioni si rimanda al profilo Linkedin.
Marco Alvise De Stefani collabora dal 2004 con il Ministero della Giustizia in Veneto e in Friuli-Venezia Giulia, dove ha seguito oltre 150 indagini. È amministratore unico di Synaptic Srls, azienda specializzata in Digital Forensics e Incident Response, e consulente tecnico di aziende e studi legali eccellenti del Friuli-Venezia Giulia. È docente di Digital Forensics in corsi di formazione per le Forze dell'Ordine, la Magistratura e gli Avvocati, per l'Università Svizzera e per seminari organizzati dall'Università degli Studi di Udine e da associazioni/enti del settore. Ha partecipato come relatore a convegni nazionali e internazionali sulla Digital Forensics e a eventi divulgativi. È autore di svariate pubblicazioni e articoli scientifici.

Abstract

E' noto che l'epoca attuale è dominata dalla tecnologia, che costituisce l'infrastruttura delle relazioni sociali.
La comunicazione, peraltro sempre più pervasiva, avviene ormai per la maggior parte attraverso strumenti tecnologici. Ciò non implica soltanto la possibilità da parte di terzi - lo Stato, i provider, altri soggetti - di manipolare il flusso informativo o di intervenire esternamente sui contenuti, ma pone una sempre maggiore difficoltà nella documentazione dei rapporti sociali. Se è vero che la documentazione, infatti, è da sempre un elemento centrale nello sviluppo della socialità umana - essa può essere intesa in senso ampio come un'attività compiuta dall'uomo per rappresentare fatti o eventi attraverso degli artefatti - e se è vero che nell'antichità questa funzione era svolta anche in modo primitivo ma efficace - si pensi ai monumenti, alle opere d'arte in generale o alla scrittura - oggi tuttavia si assiste alla smaterializzazione dei supporti su cui tali rappresentazioni sono fissate. I rapporti sociali sono documentati essenzialmente attraverso tracce informatiche ed è complicato portare a sostegno delle proprie rivendicazioni giuridiche le rappresentazioni delle vicende umane che ne costituiscono il fondamento o che ne fanno titolo (es: un'email, un messaggio WhatsApp, un SMS, un post su Facebook).
Se si considera l'ambito specifico del diritto ed in particolare il campo forense, si può osservare che le particolari caratteristiche della prova digitale impongono specifiche cautele concernenti non soltanto la fase di acquisizione bensì l'intero ciclo di utilizzo nel processo e persino la sua archiviazione al termine del giudizio. Spesso si sottovaluta che la prova digitale contiene informazioni che riguardano non solo il "cosa facciamo" (evidenze empiriche della nostra condotta come intercettazioni di comunicazioni, coordinate GPS degli spostamenti, abitudini di consumo) ma anche il "chi siamo" (tracce riproducibili di caratteri fisici come impronte digitali, registrazioni vocali, immagini). E si sottovaluta il fatto che tali informazioni sono facilmente manipolabili perché difficili da archiviare in modo definivo.
Dal punto di vista operativo il problema del "controllo" si pone come garanzia della funzionalità della prova sia rispetto all'acquisizione che alla sua gestione. Nel primo momento, infatti, la selezione del materiale da raccogliere deve tenere conto di due esigenze contrapposte: il rispetto della riservatezza dell'indagato, da una parte, e la necessità di verificare una possibile contraffazione dei dati, dall'altra. In secondo luogo, si prospetta l'opportunità di sottoporre i dati ad opportune misure di sicurezza per limitare l'accesso a quelle figure individuate dall'aspetto organizzativo e come strumento di gestione interna delle informazioni.
Nel nostro contributo si sostiene la tesi che non si può pensare di risolvere il problema della prova informatica semplicemente digitalizzando le attuali procedure o adeguandole alle tecnologie informatiche più recenti. Occorre superare l'attuale approccio, che si può chiamare genericamente "analogico", con una visione "digitale" in cui vi è sinergia tra la prova, le figure professionali che a vario titolo dispongono della prova - e quindi la "controllano" - e le regole che garantiscono i diritti dell'imputato nella dialettica tra accusa e difesa. Ciò vale ancor di più se si considera che in

ambienti cloud gli utenti – e, nelle ipotesi più avanzate, anche chi fornisce il servizio – non hanno accesso diretto ai calcolatori in cui sono memorizzate le loro risorse. In questo senso il "controllo" è solo apparente, anche per lo stesso provider.
Nel presente contributo si esaminano alcune possibili procedure per l'acquisizione forense in ambienti cloud alla luce del quadro normativo di riferimento in Unione Europea.

Prima parte

La prima parte si snoda attraverso tre punti principali. Il quarto e il quinto possono essere considerati come implicazioni del più generale problema del controllo dell'informazione.

La «Società dell'Informazione» come società dipendente dalla tecnologia
Joseph Carl Robnett Licklider e Robert W Taylor, *The Computer as a Communication Device*, in «Science And Technology», 76 (1968), pp. 21-31, p. 26.
«Mobile Lovers», di Banksy (2014)
Si pensi a come la comunicazione elettronica veniva concepita – anzi immaginata – in origine e come essa si configura attualmente.
È facile contrapporre illusioni e disillusioni.
Un esempio di questa retorica può essere data da queste due immagini. Nella prima – tratta da un contributo che è un classico nella storia della Rete - sembra che la tecnologia aiuti a «comunicare». La seconda – che è un'opera del famoso writer britannico Banksy – costituisce invece una specie di atto di condanna che l'effetto è esattamente il contrario, l'allontanamento.

The number of deaths in 2015 related to the practice of taking selfies has risen to 12 after a 66-year-old Japanese tourist, Hideto Ueda, died when collapsing and falling down stairs posing at the Taj Mahal in India. His travelling companion survived, but suffered a broken leg.
Ma «di chi è la colpa?». Non ci sono scuse, non può essere che nostra. Possiamo dire che la tecnologia non solo ci aiuta a comunicare, ma a esprimere tutte le nostre inquietudini. E lo fa in un modo molto efficiente, amplificandole a dismisura. La tecnologia «uccide?» o siamo noi a ucciderci attraverso la tecnologia? Ce lo meritiamo? È una forma perversa di «darwinismo tecnologico», per cui «sopravvivranno» solo coloro che impareranno ad adeguarsi alla tecnologia?
È «vitale» non farsi prendere la mano (e nel caso del tizio che corre davanti al toro, è proprio il caso di dirlo).

Il problema del controllo dell'informazione
Shannon, C. E., *A Mathematical Theory of Communication*, in «Bell System Technical Journal», XXVII n. 3 (1948), pp. 379-423, p. 381
In effetti tutto parte da questo principio, espresso da Shannon in questo articolo che è la base dello sviluppo delle comunicazioni elettroniche.

Un mittente, un messaggio, un destinatario. Il rumore. L'entropia da combattere, l'informazione da preservare.
Il problema del controllo dell'informazione è intrinseco nella necessità della sua trasmissione.
È connaturato, non è possibile prescinderne.

L'idea comune che vi sia una contrapposizione tra «chi vuole controllare» e «chi non vuole essere controllato» nasconde forse una verità inconfessabile: non si può «condividere» senza esporsi al «controllo».

L'idea di fondo è molto semplice: non ci si può tuffare in un mare e sperare di non bagnarsi.
Questo problema ha due implicazioni di cui si vuole parlare in questa sede:

(1) La documentazione
(2) La qualità dell'informazione

Prima conseguenza: la documentazione dei rapporti sociali
Codice di Ur-Nammu, (2100-2050 a.C.), il più antico corpus normativo conosciuto, di origine sumera
La regolarità appartiene alla natura umana. Parliamo non soltanto di disciplina delle relazioni sociali, ma anche di disciplina interiore.
Diritto e morale hanno entrambe questa caratteristica: sono un insieme di regole.
La documentazione delle norme di condotta è una delle primarie esigenze della civiltà giuridica.
Esiste un legame inscindibile tra la scrittura come tecnica di documentazione e lo sviluppo del diritto.
Possiamo pensare a una civiltà senza documenti? Senza archivi? Senza storia?
Sarebbe una civiltà primitiva.

Il problema della digitalizzazione dei documenti è evidente.
L'informazione, proprio per la sua natura, è estremamente manipolabile.
Anzi, si potrebbe dire che è informazione proprio ciò che è oggetto di controllo.
In un certo senso, la controllabilità stessa è manipolabilità di qualcosa e quindi, in linea di principio, contraddice la documentazione.
Se qualcosa può essere documentato nei confronti di qualcuno, significa che costui non ha un vero e proprio controllo – in senso tecnologico - su tale oggetto.
La documentazione è un potere in quanto tale.
È un po' la differenza tra chi sa scrivere e chi non sa scrivere, se vogliamo trasporla in una dimensione «analogica».
In base a ciò che abbiamo detto in precedenza, dunque,
IN TEORIA: condivisione = controllo -> assenza di documentazione

[la condivisione equivale al controllo e, in questo senso, determina una assenza di documentazione]
Ma allo stesso tempo si assiste a un fenomeno paradossale.
Il controllo si realizza praticamente come una forma di documentazione pervasiva e continua, da parte di Stati, providers, ma anche da parte degli altri soggetti con cui abbiamo a che fare. Basta pensare a quante persone hanno il nostro numero di cellulare in rubrica. A quanto hanno il nostro compleanno, anniversario, onomastico.
Quindi
IN PRATICA: condivisione (dei dati) -> controllo) = documentazione
[la condivisione dei dati – per dire, nei social network – determina un controllo reciproco che si identifica in una pervasiva documentazione]

Seconda conseguenza: la qualità dell'informazione
Altra implicazione è quella relativa alla qualità dell'informazione.
Consideriamo il problema sotto l'aspetto sostanziale.
Cosa si documenta? Le cose importanti? Le cose non importanti?
Esiste una contraddizione evidente, data dal fatto che le cose «troppo importanti» non vengono condivise e quindi non sono documentate (si pensi ai documenti riservati o segreti di Stati o imprese), mentre si ritiene che le cose «poco importanti» (il gossip, per dire) non meritino di essere fissate.
La documentalità riguarda una dimensione dell'essere intermedia tra questi due estremi.
Solo le informazioni «mediamente rilevanti» meritano di essere documentate.

Eppure la «qualità dell'informazione» ha anche una connotazione formalistica, che è quella più comune oggi.
Il problema riguarda il modo in cui l'informazione viene generata.
O meglio, il problema riguarda il processo di elaborazione del dato che viene preso in considerazione (tecnicamente forse bisognerebbe parlare della cosa come di una «entità osservabile»).
La questione riguarda in fondo la «filosofia della scienza», ma anche – e di questo parleremo tra poco – il problema della prova in giudizio.
Sempre di più oggi vengono utilizzate prove «informatiche» che sono una sottospecie delle prove scientifiche.
Alla necessità di utilizzare strumenti informatici (elemento oggettivo) si unisce quella di possedere competenze specifiche da parte di coloro i quali li utilizzano (elemento soggettivo).
I criteri per determinare la qualità dell'informazione sono diversi e sono ancora in evoluzione e in discussione. Nella immagine si fornisce una rappresentazione abbastanza superficiale dei principali criteri.

In questo senso, il controllo rappresenta un problema in termini di qualità dell'informazione perché solo chi controlla ha la possibilità di essere certo della qualità dell'informazione, ma proprio perché chi controlla ha la possibilità di manipolare il dato, in linea di principio la qualità della sua informazione non è credibile nel momento in cui viene condivisa con altri (che non hanno il controllo).
Chi non ha il controllo del dato non si fida di chi ce l'ha.
Non ha alcuna ragione per farlo.
O meglio, l'unica ragione che avrebbe è una scelta, un gesto di fiducia basato su criteri tendenzialmente estranei al contenuto dell'informazione.

Conoscenza = «justified true belief»
La fonte e il metodo di analisi garantiscono la veridicità dell'opinione a cui pertanto si attribuisce valore di conoscenza.
Come si nota da questa definizione di «conoscenza», in fondo si tratta sempre di una «credenza», qualcosa di cui l'interlocutore deve essere convinto da qualcun altro.

Take away

(1) «controllo» e «condivisione» sono due facce della stessa medaglia
(2) La documentazione non è un problema esclusivo della contemporaneità, ma è sempre esistito, sia pure in diverse forme
(3) La qualità dell'informazione dipende anche solo in minima parte da una fiducia nell'interlocutore

Seconda parte

Come vengono utilizzati quotidianamente i dispositivi digitali più comuni (smartphone, tablet, pc, ecc.)? Possono contenere non solo dati personali idonei a rivelare prove empiriche della nostra condotta – il "cosa facciamo" – ma anche tracce riproducibili di caratteri fisici che identificano in modo inequivocabile gli individui a cui esse si riferiscono, e quindi consentono di determinare il "chi siamo", tanto che la loro perdita o manipolazione da parte di terzi può causare danni irreparabili , soprattutto quando sono associati a dati sensibili e si riferiscono a tratti non modificabili della persona (come le impronte digitali).
L'importanza dei dati trattati non viene tenuta adeguatamente in considerazione da parte delle cancellerie dei tribunali. Generalmente il supporto originale viene conservato dall'Ufficio dei corpi di reato, spesso sigillato, cautelato, inventariato, archiviato e a disposizione unicamente del personale autorizzato al suo trattamento, previa annotazione su registri o mediante verbali di consegna e restituzione. Al contrario le copie forensi o i dati estrapolati sono spesso riversati in supporti ottici (CD, DVD, Blu-Ray) o su memorie di massa (pendrive USB, dischi fissi, ecc.) conservati nel fascicolo cartaceo, e sono a disposizione di chiunque abbia accesso al fascicolo,

spesso protetti al massimo da sigilli cautelati con firme che dopo la prima apertura non vengono più ripristinati.
Una cautela utile a diminuire il rischio di accessi abusivi e indiscriminati a una quantità elevata di dati sensibili consiste nel circoscrivere il campo d'azione direttamente nella fase di acquisizione esclusivamente agli elementi di diretto interesse per le indagini.
Tale precauzione preserverebbe certamente la riservatezza dell'indagato ma indebolirebbe l'efficienza nell'azione dell'autorità giudiziaria principalmente per due motivi. In primo luogo, non sarebbe possibile svolgere ulteriori approfondimenti dopo una prima disamina di quanto acquisito. Ad esempio, se fossero raccolti unicamente gli sms e dal loro esame emergessero riferimenti a conversazione avvenute mediante un altro servizio di messaggistica, queste ultime non potrebbero essere acquisite. In secondo luogo, bisogna ricordare che gli elementi estrapolati dal sistema che li ha generati vengono privati di una serie di informazioni potenzialmente molto importanti. Ad esempio, se da uno smartphone venisse acquisita unicamente una foto perderemmo una serie di informazioni presenti nel sistema operativo o in altre applicazioni che le sono correlate pur non facendo parte di essa, e che pertanto potrebbero confermarne o confutarne la genuinità .
Compreso che la riservatezza del dato non può essere garantita soltanto in sede di acquisizione occorre prendere in considerazione la fase successiva, che riguarda il suo trattamento.
La digital forensics comprende già uno strumento in grado di garantire la riservatezza dei dati acquisiti: la cosiddetta "catena di custodia". Essa serve a garantire la non modificabilità del dato e attiene alla preservazione del supporto originale e di quello contenente la sua copia forense; essi dovranno essere conservati adottando ogni misura più idonea a garantirne la non alterazione e la possibilità di poter effettuare, in qualsiasi momento, eventuali ulteriori controanalisi. Aspetto fondamentale sia della conservazione sia dell'acquisizione del reperto informatico consiste nella tracciabilità del suo percorso, garantita dalla produzione di idonea e puntuale documentazione attestante tutte le attività – descritte in modo dettagliato – poste in essere nel corso delle operazioni di digital forensics, documentazione che va a costituire appunto la catena di custodia.
La catena di custodia viene quindi utilizzata prevalentemente per garantire l'autenticità delle prove informatiche, l'integrità dei dati acquisiti, nonché per assicurare la continuità probatoria delle prove digitali ossia la possibilità di tenere traccia del procedimento di repertazione in ogni sua fase, dal momento del sequestro del dato informatico al momento del dibattimento, al fine di garantire l'assenza di modifiche o alterazioni per tutto il periodo dell'iter processuale.
Un aspetto spesso sottovalutato della catena di custodia è che essa può essere utilizzata anche per stabilire chi ha avuto accesso al dispositivo originale o alla copia prodotta, tutelando il rispetto della riservatezza dei dati ivi contenuti.
Una ulteriore implementazione di tale funzionalità, a ben vedere, potrebbe consentire lo sviluppo di una struttura tecnologica in cui le interazioni tra gli operatori autorizzati si coniugano con le esigenze inerenti la sicurezza dei dati, di modo che la autenticità delle informazioni veicolate all'interno del processo sarebbe tutelata attraverso le procedure che disciplinano gli accessi ai dati.

Riprendendo quanto svolto nei paragrafi precedenti, si può osservare che la prova digitale vera e propria e le informazioni relative alla conservazione del reperto si collocano su diversi "livelli di astrazione", sicché una soluzione efficace e percorribile senza stravolgere l'attuale prassi adottata può essere ottenuta implementando con maggiore rigore il "livello di astrazione" relativo agli accessi al materiale probatorio, con la piena applicazione del concetto di "catena di custodia", quindi registrando qualsiasi accesso ai supporti, sia da parte di soggetti esterni che da parte del personale delle forze dell'ordine o delle cancellerie. Dato che attualmente i supporti contenenti i dati non sono mantenuti in un apposito archivio (come avviene per i corpi di reato) ma vengono riposti all'interno del faldone contenente il fascicolo cartaceo, sarebbe opportuno utilizzare una ulteriore forma di protezione, ad esempio una cifratura robusta, possibilmente basata su software di cui possa essere garantita l'accessibilità futura anche a terzi (ad esempio open-source). Ovviamente, la password di cifratura non dovrebbe essere allegata al fascicolo, ma seguire un iter diverso e quindi verosimilmente dovrebbe collocarsi ad un diverso "livello di astrazione".
Una soluzione di più ampio respiro richiederebbe uno studio che trascende gli scopi del presente articolo, tuttavia è possibile elencare alcune delle caratteristichecheunsistemaidealeditrattamentodelleprovedigitalidovrebbe possedere alla luce delle osservazioni compiute in questa sede:

(a) i dati digitali dovrebbero rimanere in tale formato ed essere ospitati su server centralizzati, con bassi costi di mantenimento, sicurezza e garanzia di accessibilità e backup;

(b) bisognerebbe fornire accesso diretto al dato originale (copia forense o simili) e al dato "granulare" frutto dell'analisi (ad esempio, gli sms);

(c) occorrerebbe gestire gli accessi alle diverse tipologie di dati in base alla necessità e al livello di autorizzazione dell'utente (ad esempio, il perito nominato dal giudice potrebbe avere accesso alla copia forense mentre il personale di cancelleria solo ai risultati della perizia), mantenendo la registrazione degli accessi.

Sviluppi futuri
Cyber-investigation Analysis Standard Expression (CASE)
Evidence Project
Acquisizione di prove dal Cloud
L'Autorità Giudiziaria è al vaglio delle aziende.
L'opinione comune si rifiuta di consegnare i dati all'A.G. per motivi di Giustizia, ma si fida ciecamente delle aziende a cui consegna tutti i propri dati.